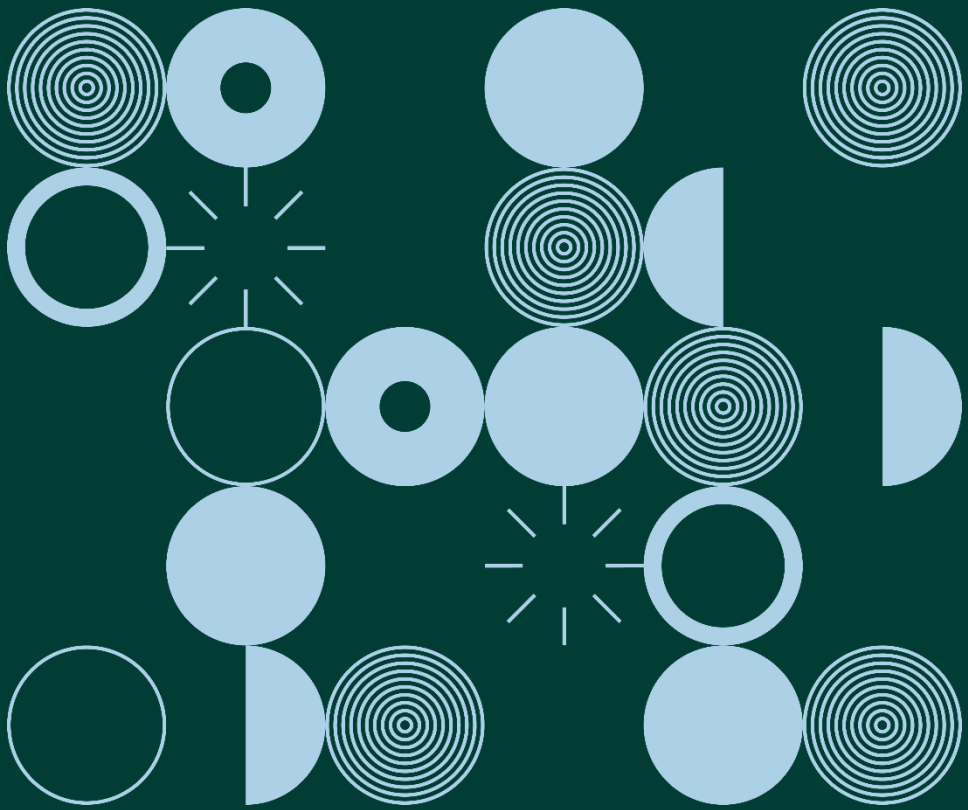
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Treoirnóta:

Treoir do Rialaitheoirí ar Shlándáil Sonraí

Feabhra 2020



Clár

Treoir do Rialaitheoirí ar Shlándáil Sonraí

Bíonn ag méadú i gcónaí ar an méid sonraí pearsanta a shealbhaíonn rialaitheoirí sonraí san earnáil phríobháideach agus san earnáil phoiblí araon faoi dhaoine aonair. Ceann de na príomhchúiseanna leis sin is ea an laghdú atá tagtha ar an gcostas a bhaineann le stóráil agus próiseáil leictreonach. Níos mó agus níos mó, bíonn eagraíochtaí ag seachfhoinsiú a bpróiseála sonraí chuig tríú páirtithe (próiseálaithe sonraí) freisin. Leanann a lán eagraíochtaí le méideanna móra sonraí pearsanta a shealbhú i bhfoirm

láimhe chomh maith – agus is minic a shealbhaítear na sonraí sin as an láithreán. Is é an toradh atá ar an méadú mór sin ar an méid sonraí pearsanta a phróiseáiltear agus a shealbhaítear ná go gcruthaítear dúshláin slándála do na heagraíochtaí a bhailíonn na sonraí. Is gá do rialaitheoirí sonraí iniúchadh rialta a dhéanamh ar na sonraí pearsanta atá ina seilbh agus ar na nósanna imeachta atá i bhfeidhm acu chun na sonraí sin a chosaint. Áirítear iad seo a leanas leis na ceisteanna ba cheart dóibh a chur le linn an iniúchta sin:

- ✓ An eol dúinn cé na cineálacha sonraí pearsanta a shealbhaímid
  - go leictreonach (lena n-áirítear sonraí nach bhfuil chomh follasach céanna, amhail íomhánna teilifíse ciorcaid iata (TCI)?
  - ar pháipéar?
- ✓ An féidir linn údar a thabhairt le bailiú na faisnéise seo?
  - Cén fáth a mbailímid í?
  - Cén úsáid a bhaintear aisti?
  - Cad iad na rioscaí?
  - Cá fhad a shealbhóimid í?
  - Cé na daoine a bhfuil rochtain acu uirthi?
  - Cé na daoine a nochtaimid leo í?
  - Cén áit a stórálfar í?
  - An sealbhaítear go slán í?
  - Conas a chuirimid na sonraí de láimh?
- ✓ Má dhéanaimid próiseáil sonraí pearsanta a sheachfhoinsiú chuig próiseálaí sonraí (soláthraí seirbhíse 'néalríomhaireachta' san áireamh), an deimhin linn go bhfuil nósanna imeachta slándála leordhóthanacha i bhfeidhm aige?

An Dlí

Cé nach leagtar amach san Acht um Chosaint Sonraí, 2018, ná sa Rialachán Ginearálta maidir le Cosaint Sonraí aon bhearta slándála sonracha nach mór do rialaitheoir sonraí nó do phróiseálaí sonraí a bheith i bhfeidhm acu, leagtar amach i Rialacháin na gComhphobal Eorpach (Líonraí agus Seirbhísí Cumarsáide Leictreonaí) (Príobháideachas agus Cumarsáid Leictreonach), 2011, roinnt ceanglas a bhaineann go sonrach leis an earnáil seirbhísí cumarsáide leictreonaí. Beag beann air sin, is amhlaidh go leagtar leis an Rialachán Ginearálta (Airteagail 25 agus 32) oibleagáid ar rialaitheoirí agus ar phróiseálaithe cosaint sonraí d'aon turas agus mar réamhshocrú agus 'bearta iomchuí teicniúla agus eagraíochtúla' a chur chun feidhme chun leibhéal slándála a áirithiú is iomchuí don riosca lena mbaineann, agus aird á tabhairt acu ar na nithe seo a leanas:

- an úrscothacht;
- na costais a bhaineann le cur chun feidhme;
- cineál, raon feidhme, comhthéacs agus críocha na próiseála; agus
- dóchúlacht agus déine an riosca sin maidir le cearta agus saoirsí daoine aonair.

Moltar ina dhiaidh sin sa Rialachán Ginearálta an liosta táscach seo a leanas de bhearta iomchuí:

- ainm bréige a chur i bhfeidhm agus criptiú a dhéanamh i ndáil le sonraí pearsanta;
- an cumas rúndacht leanúnach, sláine, infhaighteacht agus athléimneacht na gcóras agus na seirbhísí próiseála a áirithiú;
- an cumas infhaighteacht agus rochtain ar shonraí pearsanta a athshlánú ar mhodh tráthúil sa chás ina dtarlaíonn teagmhas fisiciúil nó teicniúil; agus
- próiseas chun tástáil, measúnú agus meastóireacht rialta a dhéanamh ar éifeachtúlacht na mbeart teicniúil agus eagraíochtúil chun slándáil na próiseála a áirithiú.

Tá oibleagáid ar rialaitheoirí sonraí agus ar phróiseálaithe sonraí a áirithiú freisin go mbeidh a mbaill foirne agus "daoine eile ag an áit oibre" ar an eolas faoi na bearta slándála atá ar bun agus go gcomhlíonfaidh siad na bearta sin. Is maidir le gach rialaitheoir sonraí agus gach próiseálaí sonraí, is cuma cén mhéid atá iontu, atá feidhm ag an oibleagáid dhlíthiúil chun sonraí pearsanta a choinneáil slán.

Sa treoirnóta seo, sainaithnímid saincheisteanna áirithe ar cheart do rialaitheoirí sonraí agus do phróiseálaithe sonraí breithniú a dhéanamh orthu le linn dóibh a mbeartais slándála a fhorbairt.

Beartais Maidir le Bailiú agus Coinneáil Sonraí

Is é an bealach is éifeachtaí chun maolú a dhéanamh ar an mbaol go gcaillfí nó go ngoidfí sonraí pearsanta ná gan na sonraí sin a shealbhú sa chéad áit. I ngach cás, ba cheart coinneáil agus macasamhlú sonraí a mheas in aghaidh an riachtanais ghnó agus iad a íoslaghdú, trí gan aon sonraí neamhriachtanacha a bhailiú nó trí shonraí a scriosadh a luaithe nach mbeidh siad ag teastáil a thuilleadh. Tá rioscaí slándála ag gabháil le haon sonraí pearsanta a choinneáil. Sampla de sin is ea cásanna ina ndéanann eagraíochtaí lánsonraí cárta creidmheasa, lena n-áirítear dáta éaga agus uimhir CVV an chárta, a bhailiú de láimh agus ina stórálann siad an fhaisnéis sin tar éis an t-idirbheart a phróiseáil.

Ba cheart do rialaitheoir sonraí a bheith ar an eolas i ngach cás faoi cé na sonraí a shealbhaíonn sé, faoi cén áit a sealbhaítear na sonraí agus faoi conas a shreabhann na sonraí tríd an eagraíocht. Gan an méid maoirseachta sin, beidh sé deacair sonraí pearsanta a chosaint go héifeachtach laistigh den eagraíocht.

Tá próiseálaithe sonraí faoi réir na n-oibleagáidí slándála céanna agus atá rialaitheoirí sonraí. Dá bhrí sin, cumhdaítear próiseálaithe sonraí le haon tagairtí do 'rialaitheoirí

sonraí' sa treoirnóta seo, ach amháin i gcás go dtugann an comhthéacs a mhalairt le fios.

Rialú Rochtana

Tá dualgas ar rialaitheoir sonraí teorainn a chur leis an rochtain ar shonraí pearsanta ar bhonn riachtanais. Ba cheart feidhm a bheith ag teorainneacha níos mó le rochtain nó ag rialuithe níos mó ar rochtain maidir le sonraí níos íogaire. Ní mór do rialaitheoirí sonraí bheith ar an eolas faoi na húsáideoirí difriúla a fhaigheann rochtain ar a gcórais/a dtaifid agus faoi na riachtanais atá ag na húsáideoirí sin. D'fhéadfadh go n-áireofaí na húsáideoirí seo leis na cineálacha difriúla úsáideora:

- baill foirne ar leibhéil éagsúla sinsearachta, oibríochta nó freagrachta;
- conraitheoirí/próiseálaithe sonraí tríú páirtí;
- custaiméirí; agus
- comhpháirtithe gnó

Ní mór breithniú a dhéanamh ar na riachtanais dhifriúla atá ag gach ceann de na cineálacha sin úsáideora agus ba cheart na pribhléidí atá acu chun rochtain a fháil ar shonraí pearsanta a bheith ag teacht go hiomlán leis na riachtanais sin.

Ba cheart an cineál rochtana a thugtar d'úsáideoir aonair a shocrú agus a athbhreithniú ar bhonn rialta. Ba cheart do bhaill foirne aonair, i measc nithe eile, rochtain a bheith acu ar na sonraí sin a theastaíonn uathu chun a ndualgais a chomhlíonadh agus ar na sonraí sin amháin, cosc a chur le húsáid a bhaint as dintiúir chomhroinnte (an t-aon ainm úsáideora amháin agus an t-aon phasfhocal amháin a bheith á n-úsáid ag níos mó ná duine amháin), agus chun úsáid pasfhocal réamhshocraithe a bhrath. Teastaíonn nósanna imeachta sonracha, ar a dtugtar beartas um "daoine a aistríonn, a fhágann agus a thagann isteach" ó na heagraíochtaí go léir a bhfuil rochtain acu ar shonraí pearsanta chun socrú cathain an rochtain roimhe a choinneáil, a mhéadú nó a shrianadh i gcás go n-athraítear ról úsáideora. Caithfear tacú le rialú rochtana trí athbhreithnithe rialta a dhéanamh chun a áirithiú gur riachtanach go dian atá an rochtain údaraithe ar fad ar shonraí pearsanta agus go bhfuil údar léi le haghaidh feidhm a chomhlíonadh.

Ba cheart aird ar leith a thabhairt ar úsáid na gcuntas riarthóra TF a bhfuil rochtain neamhshrianta acu ar shonraí pearsanta. Ba cheart beartais a bheith i bhfeidhm maidir le grinnfhiosrú agus maoirseacht a dhéanamh ar na baill foirne sin a dtugtar na cuntais sin dóibh. Ba cheart do bhall foirne a bhfuil na freagrachtaí sin air/uirthi cuntas úsáideora agus cuntas riarthóra ar leith a bheith aige/aici. Is dócha gur cheart go mbeadh leor leibhéil fíordheimhnithe ann má tá ardrochtain nó rochtain breise ag

riarthóirí ar shonraí pearsanta nó má tá rochtain nó smacht acu ar shonraí cuntais nó ar shonraí slándála duine eile.

Ba cheart rialuithe diana a bheith ann maidir leis an gcumas chun sonraí pearsanta a íoslódáil ó na córais de chuid eagraíochta. Is féidir bac a chur le híoslódáil den sórt sin trí mhodhanna teicniúla (tiomántáin a dhíchumasú, limistéir líonra nó deighleáin líonra a aonrú, i measc nithe eile). Rinne a lán eagraíochtaí an cinneadh bac a chur leis an rochtain ar phoirt USB tar éis dóibh scrúdú a dhéanamh ar na rioscaí dúchasacha a bhaineann le poirt den sórt sin a fhágáil oscailte do gach úsáideoir mar réamhshocrú.

Fíordheimhniú Rochtana

Ba cheart d'úsáideoirí aitheantóir uathúil (amhail pasfhocal, pasfhrása, cárta cliste nó ceadchomhartha eile) a bheith acu chun cead a thabhairt dóibh sonraí pearsanta a rochtain. Ní ach samplaí iad seo, agus ní liosta iomlán é; mar shampla, d'fhéadfaí úsáid a bhaint as sonraí bithmhéadracha (mar shampla, méarlorg, guth nó scanadh reitine) mar aitheantóir uathúil domhanda chomh maith. É sin ráite, cé go spreagann sonraí bithmhéadracha féin ceisteanna tromchúiseacha maidir le cosaint sonraí agus príobháideachas, ní cheart smaoineamh ar iad a úsáid ach amháin nuair is léir go bhfuil modhanna eile fíordheimhnithe easnamhach.

Pasfhocail/Pasfhrásaí

Is focal nó teaghrán carachtar iad pasfhocail. Ba cheart dhá charachtar déag ar a laghad a bheith ar áireamh i bpasfhocal láidir (dá fhad atá an pasfhocal is deacra do ríomhaire é a oibriú amach) agus d'fhéadfadh ceann amháin nó níos mó de na nithe seo a leanas a bheith ar áireamh iontu:

- ✓ litreacha (cás uachtair agus cás íochtair);
- ✓ siombailí (e.g. &, *, @, €, $ etc);
- ✓ uimhreacha (0 - 9);
- ✓ poncaíocht (?, ", !)|
- É sin ráite, níl aon gá d'úsáideoirí meascán de go leor cineálacha carachtar, mar is féidir pasfhocal láidir a chruthú le cineál amháin carachtar (m.sh. litreacha) má tá sé fada go leor agus deacair chun oibriú amach (do ríomhairí do dhaoine araon). Ba cheart pasfhocail a bheith measartha furasta le cuimhneamh don úsáideoir agus a bheith an-doiligh le tuar d'aon duine eile. D'fhéadfadh na nithe seo a leanas bheith i gceist le samplaí: M1_s?n, "The_Av1at#r"! (bunaithe ar 'My son, "the aviator"!', áit a gcuirtear carachtair randamacha in ionad gutaí áirithe nó litreacha eile)
- Te@m5Rb@dp@55word5 (55word5 (bunaithe ar 'Teams are bad passwords', áit a gcuirtear uimhreacha agus siombailí in ionad litreacha áirithe))

Ná húsáid na samplaí sin mar phasfhocail iarbhír!

Níor cheart go mbeadh luachanna i do phasfhocal a bhfuil fios go n-úsáidtear iad go minic nó go mbeifí ag súil leo a úsáid i bpasfhocail. Níor cheart úsáid a bhaint as luachanna a cuireadh i mbaol iad ach oiread. Mar shampla, d'fhéadfaí go gcuirfear bac ar úsáideoirí úsáid a bhaint as pasfhocail cosúil le:

- Pasfhocail a bhfuarthas ó sháruithe roimhe seo;
- Focail ón bhfoclóir;
- Carachtair atá athráiteach nó seicheamhach (m.sh. 'aaaaaa', '1234abcd');
- Focail sainábhair; ar nós ainm na seirbhíse, an t-ainm úsáideora, nó díorthaigh dóibhsan.

Tá pasfhrásaí cosúil le pasfhocail, ach seasann siad d'abairt nó do sheicheamh focal. Ba cheart fiche carachtar nó níos mó a bheith ar áireamh iontu agus d'fhéadfadh siombailí, uimhreacha agus comharthaí poncaíochta a bheith ar áireamh iontu freisin, mar shampla:

- "I Love the musical, The Sound of Music 2!"
- Ilike2swim@thelocalswimingpool

Ba cheart do rialaitheoirí sonraí castacht agus fad na bpasfhocal a fhorfheidhmiú, mar shampla, trí rialacha a chinntíonn nach glacfar le pasfhocail laga agus pasfhocail a athúsáidtear. Níor cheart go mbeadh ar úsáideoirí a bpasfhocal nó a bpasfhrása athrú gan chúis (m.sh. rómhinic) mar, i ndáiríre, is féidir slándáil pasfhocal a laghdú leis seo (mar shampla, trí bheith ag brath níos mó ar phasfhocail simplí nó ar phasfhocail a athúsáid). Ba cheart go n-iarrfar ar úsáideoirí a bpasfhocal nó a bpasfhrása a athrú, áfach, má tá fianaise ann gur cuireadh i mbaol é nó gur nochtadh é, nó nuair atá athrú eile maidir le riosca. Níor cheart do rialaitheoirí sonraí pasfhocail úsáideoirí a stóráil riamh mar ghnáth-théacs ach ba cheart go mbainfidh said úsáid as haiseáil chripteagrafacha atá láidir agus do-aisiompaithe chun na pasfhocail a chosaint agus chun seiceáil shábháilte a ligean le haghaidh cuspóirí logála isteach.

Ba cheart do rialaitheoirí sonraí a áirithiú go gcuirfear úsáideoirí ar an eolas gurb uathúil dóibh atá a bpasfhocal/a bpasfhrása agus nach ceadmhach é a nochtadh d'aon duine eile. Níor cheart dintiúir chomhroinnte (nuair a úsáideann úsáideoirí iomadúla an logáil isteach céanna agus an pasfhocal céanna) a cheadú am ar bith. Níor cheart réamhshocruithe arna soláthar ag díoltóirí le haghaidh pasfhocail chórais agus paraiméadair eile shlándála a fhágáil i bhfeidhm am ar bith. Ní mór do rialaitheoirí sonraí a áirithiú go gcloífidh eagraíochtaí comhpháirtíochta a bhfuil rochtain acu ar a gcórais nó ar a sonraí leis na rialuithe sin.

Nuair is féidir, ba cheart do rialaitheoirí sonraí éagsúlacht a spreagadh le pasfhocail trí na rioscaí a bhaineann le pasfhocail a athúsáid i seirbhísí eile idirlín a chur i gcuimhne d'úsáideoirí.

Fíordheimhniú Ilfhachtóra

Is é atá i gceist le fíordheimhniú ilfhachtóra (MFA) ná nuair a úsáidtear níos mó ná fachtóir amháin aitheantais le haghaidh fíordheimhniú rochtana. Baineann go leor seirbhísí úsáid as an rogha '2FA' go minic. Léiríonn sé seo go n-úsáidtear dhá fhachtóir le haghaidh fíordheimhniú. Mar shampla, in ionad úsáid a bhaint as pasfhocal a roghnaigh an úsáideoir, d'fhéadfadh sé nó sí socrú go seolfar paschód chuig seoladh ríomhphoist, uimhir fóin, nó feist eile. D'fhéadfadh go seolfar an paschód seo ó fhachtóir ar nós cainéal bithmhéadrach (m.sh. scanóir méarloirg) nó cainéal cumarsáide "seachbhanda" nó cainéal eile cumarsáide. Tabhair faoi deara, áfach, go bhfuil roinnt de na cainéil thánaisteacha seo níos sábháilte ná a chéile.

Is féidir feistí ar nós cártaí cliste nó ceadchomharthaí a úsáid mar chuid de MFA chun fíordheimhniú a thabhairt trí chód a ghiniúint lena chur isteach nó trí shlis a chuimsiú lena bhfíordheimhnítear leis an gcóras a bhfuil rochtain á fáil air. D'fhéadfadh siad uimhir aitheantais phearsanta a ghiniúint atá bailí ar feadh tréimhse an-ghairid ama. Baintear úsáid as an uimhir sin i dteannta ainm úsáideora agus pasfhocail chun an t-úsáideoir a fhíordheimhniú, agus is féidir leis an riosca ionsaithe 'lántrialacha' ar phasfhocail nó ionsaithe ina goideadh pasfhocail.

Spárálaithe Uathoibríocha Scáileáin

Ceadaítear leis an gcuid is mó de chórais do ghníomhachtú spárálaithe scáileáin tar éis tréimhse neamhghníomhaíochta ar ríomhaire, áit a n-éilítear pasfhocal chun rochtain a athbhunú. Is úsáideach atá an gníomhachtú uathoibríoch glasála sin mar nach mór don úsáideoir gníomh dearfach a dhéanamh gach uair a fhágann sé/sí an ríomhaire gan aon duine ina bhun i gcás nach mór stáisiún oibre a ghlasáil de láimh.

Beag beann ar an modh a n-úsáideann eagraíocht é, ba cheart ríomhairí a bheith glasáilte nuair nach bhfuil aon duine ina mbun. Ní hé amháin go mbaineann sé sin le ríomhairí atá i limistéir phoiblí ach baineann sé le gach ríomhaire freisin. Ní fiú córas rialaithe rochtana a bheith i bhfeidhm más rud é gur féidir le ball foirne ar bith rochtain a fháil ar ríomhairí nach bhfuil aon duine ina mbun, nó má úsáidtear pasfhocal comhroinnte.

Criptiú

Is é is criptiú ann ná an próiseas um fhaisnéis a stóráiltear ar fheiste a ionchódú agus is féidir leis a bheith ina chiseal úsáideach eile slándála. Meastar é a bheith ina bheart éigeantach slándála i gcás go stóráiltear sonraí pearsanta ar fheiste iniompartha nó i gcás go dtarchuirtear sonraí pearsanta thar líonra poiblí. Faoi mar atá amhlaidh i gcás pasfhocal, ní fiú an beart sin a dhéanamh mura gcoinnítear sábháilte an eochair a theastaíonn chun na sonraí a dhíchriptiú. Ba cheart an eochair na caighdeáin chastachta a theastaíonn le haghaidh pasfhocal mar a phléitear thuas a chomhlíonadh.

Mar thoradh ar an dul chun cinn teicneolaíochta a bheith chomh mear sin, ní féidir a bheith saintreorach maidir leis an gcaighdeán criptiúcháin lena n-áiritheofaí nach mbeadh daoine aonair neamhúdaraithe in ann sonraí a rochtain. I láthair na huaire, ghlacfaí le criptiú diosca iomláin 256 ghiotán mar chaighdeán inghlactha. Aithnímid go bhfuil roghanna eile á dtabhairt ar aghaidh ag an margadh chun criptiú sábháilte a dhéanamh ar shonraí a bhféadfadh nach mbeadh criptiú diosca iomláin ag teastáil ina leith agus a bheadh in ann an toradh slándála céanna a bhaint amach dá n-úsáidfeadh an t-úsáideoir i gceart iad.

Bogearraí Frithvíris

Ní hé amháin go dteastaíonn bogearraí frithvíris chun ionfhabhtuithe ón Idirlíon (ionfhabhtuithe trí ríomhphost nó ionfhabhtuithe ón nGréasán araon) a chosc ach teastaíonn siad freisin chun víris a d'fhéadfadh teacht as feistí iniompartha amhail méaróga cuimhne (ar cheart a n-úsáid a theorannú go docht) a chosc. Níl aon phacáiste frithvíris in ann gach ionfhabhtú a chosc mar nach nuashonraítear iad ach amháin mar fhreagairt d'ionfhabhtuithe. Tá sé ríthábhachtach go nuashonraítear bogearraí den sórt sin ar bhonn rialta agus go dtacaíonn na beartais le faireachas ó thaobh bagairtí féideartha de. Bealach úsáideach is féidir ionfhabhtuithe a chosc is ea beartas á shonrú nár cheart ceangaltáin ríomhphoist ó fhoinsí nach rabhthas ag coinne leo a oscailt.

Ballaí Dóiteáin

Tá balla dóiteáin ina bhunriachtanas i gcás go bhfuil aon nascacht sheachtrach ann, bíodh sí chuig líonraí eile nó chuig an Idirlíon. Tá sé tábhachtach go gcumraítear ballaí dóiteáin i gceart mar gur uirlis ríthábhachtach iad le haghaidh iarrachtaí rochtain neamhúdaraithe a fháil a chomhrac. Tá méadú tagtha ar a thábhachtaí atá ballaí dóiteáin mar go mbíonn ag méadú ar an méid a bhaineann eagraíochtaí agus daoine aonair úsáid as naisc Idirlín atá "curtha air de shíor", rud a fhágann go bhfuil siad i mbaol méadaithe ionsaí.

Paisteáil Bogearraí

Is iad paistí na nuashonruithe is déanaí ó chruthaitheoir do bhogearraí córas oibriúcháin nó do bhogearraí feidhmchláir. De ghnáth, cuimsítear iontu deisiúcháin ar ábhair imní fhéideartha slándála agus is féidir leo a bheith ina n-uirlis thábhachtach le haghaidh cosc a chur ar haiceáil nó ar ionsaithe bogearraí mailíseacha. Ba cheart d'eagraíochtaí a áirithiú go bhfuil nósanna imeachta bainistíochta paistí atá rialta, comhsheasmhach agus cuimsitheach i bhfeidhm acu.

Nuair is féidir, sula suiteáiltear na paistí is déanaí, is dea-chleachtas é na paistí sin a shuiteáil i dtimpeallacht tástála chun a áirithiú nach gcruthóidh na paistí aon fhadhbanna eile le do chórais. Ba cheart taifead a choinneáil den dáta agus den phaiste a suiteáladh ar chóras freisin.

Cianrochtain

I gcás go gceadaítear do bhall foirne/do chonraitheoir rochtain a fháil ar an líonra ó láthair chian (e.g. ón mbaile nó ó chuairt as an láithreán), cruthaíonn an rochtain sin laige fhéideartha sa chóras, go háirithe nuair a fhaightear an rochtain ó líonra gan sreang. Chuige sin, ba cheart an gá leis an rochtain sin a mheasúnú go cuí agus ba cheart bearta slándála a athmheasúnú sula ndeonaítear cianrochtain. Más féidir déanamh amhlaidh, níor cheart an rochtain a thabhairt ach amháin do sheoltaí sonracha IP. Ba cheart tús áite a thabhairt do shlándáil nuair atá rochtain á deonú d'eagraíochtaí comhpháirtíochta.

Gnéithe tábhachtacha den riosca sin a bhainistiú iad bearta slándála teicniúla, measúnuithe slándála, comhaontuithe conarthacha atá ar aon dul le ceanglais an Rialacháin Ghinearálta maidir le Cosaint Sonraí agus le ceanglais an Achta um Chosaint Sonraí, 2018, agus caighdeáin chomhaontaithe um bainistíocht sócmhainní comhroinnte. Tá sé mar fhreagracht ar an rialaitheoir sonraí a áirithiú nach féidir slándáil an chórais a chur i mbaol, beag beann ar an modh trína bhfaigheann úsáideoir cianrochtain ar a c(h)óras. Ba chóir cuimhneamh ar fhíordheimhniú ilfhachtóra le haghaidh a léithéid de rochtain sa chomhthéacs seo.

Líonraí Gan Sreang

Is féidir líonra a fhágáil neamhchosanta ar ionsaí i gcás go bhfaightear rochtain ar fhreastalaí trí nasc gan sreang. Is féidir leis an timpeallacht fhisiciúil ina n-oibrítear córais den sórt sin a bheith ina toisc nuair atáthar ag déanamh amach an bhfuil nó nach bhfuil laigí ann i slándáil an chórais. Faoi mar atá amhlaidh i gcás cianrochtana, ba cheart líonraí gan sreang a mheasúnú ar fhorais slándála in ionad iad a mheasúnú ar

bhonn a n-éascaíochta úsáide ina haonar. Ní mór do rialaitheoirí sonraí a áirithiú go bhfuil slándáil leordhóthanach i bhfeidhm ar an líonra trí bhearta cuí criptiúcháin a dhéanamh nó trí fheistí údaraithe a shonrú, mar shampla.

Tá leochaileachtaí ar leith bainteach le húsáid a bhaint as líonraí WiFi gan slándáil de chuid tríú páirtithe (e.g. na líonraí sin a chuirtear ar fáil in aerfoirt agus in óstáin, i measc nithe eile). Is féidir le feiste a úsáideann líonra den sórt sin bheith neamhchosanta ar ionsaithe a dhéantar ó mheaisíní eile ar an líonra. Ba cheart dea-bhalla dóiteáin a shuiteáil ar an bhfeiste iniompartha chun ionsaithe den sórt sin a chosc. Níor cheart an fheiste a nascadh leis an líonra ach amháin nuair is gá. Nuair atá WiFi gan slándáil á úsáid chun sonraí pearsanta nó sonraí íogaire a tharchur, ba cheart seisiún sábháilte Gréasáin a bheith i bhfeidhm chun na sonraí a chosaint.

Feistí Iniompartha

Is leochaileach go háirithe i leith gadaíochta agus caillteanas de thimpiste atá ríomhairí glúine, méaróga cuimhne, fóin chliste agus cineálacha eile feiste iniompartha. I gcás go measann rialaitheoir sonraí gur gá sonraí pearsanta a stóráil ar fheiste iniompartha, ba cheart an fheiste sin a bheith criptithe. Ba cheart criptiú diosca iomláin a úsáid chun maolú a dhéanamh ar stóráil comhad lasmuigh de dheighleán criptithe den diosca.

I gcás fóin chliste, ba cheart pasfhocal láidir a éileamh ar chumrú agus tar éis neamhghníomhaíocht a mhaireann roinnt nóiméad freisin. I gcás go gcaillteár feiste den sórt sin, ba cheart bearta a dhéanamh lom láithreach chun a áirithiú go ngníomhachtófar an tsaoráid cianghlanta cuimhne. Ba cheart do bhaill foirne a leithdháiltear feistí den sórt sin orthu bheith ar an eolas faoi na nósanna imeachta ábhartha.

Logaí agus Rianta Iniúchóireachta

Bainfear an bonn ó chórais rialaithe rochtana agus ó bheartais slándála mura féidir leis an gcóras mí-úsáidí a shainaithint. Dá bharr sin, ba cheart córas a bheith in ann an t-ainm úsáideora a fuair rochtain ar chomhad agus am na rochtana sin a shainaithint. Ba cheart loga a chruthú freisin de na hathruithe a rinneadh, mar aon le hainm an údair/an eagarthóra.

Is féidir logaí agus rianta iniúchóireachta a úsáid chun cabhrú leis an gcóras slándála a riar go héifeachtach agus is féidir leo tabhairt ar bhaill foirne gan mí-úsáid a bhaint as an gcóras. Ba cheart a chur in iúl don fhoireann go bhfuil logáil i bhfeidhm agus go n-athbhreithnítear logaí úsáideora go rialta. Ní hé amháin gur cheart díriú a leagan i bpróisis faireacháin ar líonraí, ar chórais oibriúcháin, ar chórais bhraite ionróirí agus ar

bhallaí dóiteáin, ach ba cheart seirbhísí cianrochtana, feidhmchláir Ghréasáin agus bunachair shonraí a chur ar áireamh iontu freisin. Is féidir le córais logála go leor faisnéise a ghiniúint agus, chun iad a úsáid go héifeachtach, is dócha go gcabhródh modh uathoibríoch ar nós Monatóir Teagmhais Córais Faisnéise (SIEM) chun scagadh a dhéanamh agus chun foireann slándála a chur ar a n-airdeall faoi iontrálacha neamhrialta rianta iniúchta.

Gníomhaíonn córas braite ionróirí mar chóras inmheánach aláraim a dhéanann faireachán ar ghníomhaíochtaí mailíseacha ar líonra nó ar chóras agus a thugann tuairisc orthu. Aidhm eile atá le córais den sórt sin is ea ionsaithe a dhéantar ó áiteanna laistigh den chóras a bhrath. Ba cheart d'aon eagraíocht a phróiseálann méideanna móra sonraí pearsanta córas braite ionróirí a bheith in úsáid agus gníomhachtaithe aige. I gcás go ngintear foláirimh/imeachtaí le haon chórais den sórt sin, ní mór córas fiúntach a bheith i bhfeidhm chun iad a scrúdú ar bhealach tráthúil. Is é an aidhm atá leis sin go gcabhrófar le gníomhaíocht neamhghnách a shainaithint agus go ndéanfar beart ceartaitheach lom láithreach má tá sárú leanúnach slándála ann.

Córais Chúltaca

Tá córas cúltaca ina mhodh bunriachtanach le haghaidh athshlánú tar éis sonraí a chailleadh nó a léirscriosadh. Cé gur cheart córas de chineál éigin a bheith i bhfeidhm, beidh minicíocht agus cineál an chúltaca ag brath ar an gcineál eagraíochta agus ar chineál na sonraí atá á bpróiseáil, i measc nithe eile. Is ionann na caighdeáin slándála do shonraí cúltaca agus na caighdeáin slándála sin do shonraí beo.

Pleananna Freagartha do Theagmhais

Is féidir le meancóga teacht chun cinn am ar bith, fiú má úsáidtear na córais is fearr dearadh. Mar chuid de bheartas slándála sonraí, ba cheart d'eagraíocht bheith ar an eolas faoi cad a dhéanfadh sí i gcás sárú sonraí chun go mbeidh sí réidh le freagairt. Seo iad roinnt ceisteanna a d'fhéadfá do mhachnamh a dhéanamh orthu:

- ✓ Cad a dhéanfadh d'eagraíocht i gcás teagmhas sárú sonraí?
- ✓ An bhfuil beartas i bhfeidhm ag d'eagraíocht ina sonraítear cad is sárú sonraí ann? (Ní fholaíonn sé méaróga cuimhne/dioscaí/ríomhairí glúine caillte amháin. D'fhéadfadh go bhfolódh sé freisin cailleadh an rialaithe ar shonraí pearsanta a chuirtear de chúram ar eagraíochtaí, lena n-áirítear rochtain mhíchuí ar shonraí pearsanta ar chórais na heagraíochta nó seoladh sonraí pearsanta chuig na daoine míchearta).

- ✓ Conas a bheadh a fhios agat gur fhulaing d'eagraíocht sárú sonraí? An dtuigeann foireann na heagraíochta (ar gach leibhéal) na himpleachtaí a ghabhann le sonraí pearsanta a chailleadh?
- ✓ Ar shonraigh d'eagraíocht cé na daoine ar cheart do bhaill foirne dul i dteagmháil leo má chaill siad rialú ar shonraí pearsanta?
- ✓ An dtugtar mionsonraí soiléire i mbeartas na heagraíochta faoi cé atá freagrach as déileáil le teagmhas?
- ✓ An gcumhdaítear le beartas d'eagraíochta na ceanglais um thuairisciú éigeantach sáruithe (nuair is infheidhme) faoin Acht um Chosaint Sonraí, 2018, faoin Rialachán Ginearálta maidir le Cosaint Sonraí, agus/nó faoi na Rialacháin Ríomhphríobháideachais (I.R. Uimh. 336 de 2011) (riachtanais nua inúsáidteachta agus athléimneachta san áireamh)?

Fáil Réidh de Threalamh

Nuair a fhaigheann siad réidh de threalamh atá as feidhm nó nach bhfuil ag teastáil a thuilleadh, tugann a lán rialaitheoirí sonraí deis don fhoireann an trealamh a cheannach nó deonaíonn siad do charthanais iad. Tá sé mar fhreagracht ar an rialaitheoir sonraí a áirithiú go ndearnadh na sonraí go léir a stóráladh roimhe sin ar na feistí a bhaint sula bhfaightear réidh díobh. Ní leor tiomántáin chrua na bhfeistí a fhormáidiú amháin mar gur féidir na sonraí a aisghabháil fós. Tá bogearraí ar fáil le haghaidh ábhar an tiomántáin chrua a fhorscríobh le sraith uimhreacha 1 agus 0 chun a áirithiú nach mbeifear in ann sonraí roimhe a aisghabháil. Ag brath ar chineál na sonraí a stóráiltear, moltar go bhforscríobhfaí tiomántáin chrua idir trí huaire agus cúig huaire.

I gcás nach bhfuil na feistí á n-athchúrsáil/á n-athúsáid, is féidir na tiomántáin chrua a scriosadh go fisiciúil nó a dhíghabhsáil (modh chun sonraí a léirscriosadh ó fheiste stórála maighnéadaí).

Tá sé tábhachtach breithniú a dhéanamh ar na cineálacha difriúla trealaimh a bhféadfadh go mbeadh sonraí pearsanta orthu. Seachas na samplaí soiléire amhail freastalaithe, ríomhairí agus ríomhairí glúine, is ann do roinnt feistí eile a bhféadfadh go stórálfaí sonraí pearsanta orthu. D'fhéadfadh go n-áireofaí leo fóin chliste, fótachóipeálaithe digiteacha agus meaisíní facsála, i measc nithe eile. Ní mór aon sonraí a stóráiltear ar na feistí sin a léirscriosadh freisin sula bhfaightear réidh díobh.

Slándáil Fhisiciúil

Chomh maith le bearta slándála teicniúla, caithfidh rialaitheoirí sonraí smaoineamh ar na bearta slándála fisiciúla atá riachtanach chun slándáil agus sláine aon sonraí pearsanta a phróiseálann siad a chinntiú. Agus iad ag déanamh measúnú ar riachtanais

slándála fisiciúla, ba cheart do rialaitheoirí sonraí smaoineamh ar roinnt cosaintí, lena n-áirítear, ach gan a bheith teoranta le:

- slándáil imlíne (faireachán a dhéanamh ar rochtain, an oifig a bheith glasáilte agus faoi aláram nuair nach bhfuil sí in úsáid);
- srianta ar rochtain ar limistéir íogaire laistigh den fhoirgneamh (amhail seomraí freastalaí);
- láthair an ríomhaire (chun nach mbeidh daoine den phobal in ann amharc ar an scáileán);
- stóráil comhad (comhaid gan a bheith stóráilte i limistéir phoiblí agus rochtain gan a bheith ar fáil ach amháin do na baill foirne a dteastaíonn uathu comhaid ar leith a rochtain); agus
- fáil réidh de thaifid go sábháilte (sonraí a stóráiltear go leictreonach a "ghlanadh" go héifeachtach; fáil réidh de thaifid pháipéir go sábháilte).

An Toisc Dhaonna

Beag beann ar na rialuithe teicniúla nó fisiciúla a chuirtear ar chóras, is é an beart slándála is tábhachtaí ná a áirithiú go mbíonn baill foirne ar an eolas faoi na freagrachtaí atá orthu. Níor cheart pasfhocail a scríobh síos agus a fhágáil in áiteanna áisiúla; níos cheart pasfhocail a chomhroinnt i measc comhghleacaithe; níor cheart ceangaltáin ríomhphoist nach rabhthas ag coinne leo a oscailt gan iad a scagthástáil le bogearraí frithvíris ar dtús. Modh éifeachtach cosanta in amanna is ea oiliúint éifeachtach a chur ar fhostaithe sna rioscaí a bhaineann le sonraí a chur i gcontúirt, ina ról maidir leis an méid sin a chosc agus i bhfreagairt a thabhairt i gcás fadhbanna. I gcás a lán eagraíochtaí, socraíonn siad beartais slándála agus nósanna imeachta slándála ach teipeann orthu iad a chur chun feidhme go comhsheasmhach. Chun cuidiú le hoiliúint éifeachtach, d'fhéadfaí seisiúin oiliúna a chur ar fáil atá bunaithe ar shuíomhanna féideartha.

Cuid thábhachtach de chóras ar bith a bhfuil mar aidhm leis sonraí pearsanta a chosaint iad rialuithe atá dírithe ar chuntasacht an duine aonair agus na heagraíochta agus a áirithiú go gcomhlíonfar na beartais. Aithnigh rialuithe éigeantacha ar dtús agus déan cinnte de go gcuirtear na rialuithe sin chun feidhme ar fud na heagraíochta gan aon eisceacht. A luaithe atá siad i bhfeidhm, bog ar aghaidh chuig rialuithe níos sofaisticiúla a bhfuil mar aidhm leo maolú a dhéanamh ar na rioscaí atá sonrach don eagraíocht agus don chineál sonraí/do na cineálacha sonraí a phróiseáiltear.

Ní mór do rialaitheoirí sonraí nósanna imeachta a bheith i bhfeidhm acu chun athrúchán foirne a bhainistiú, lena n-áirítear feistí stórála sonraí a fháil ar ais agus ceadanna rochtana a bhaint go mear.

Deimhniú

Is féidir le deimhniú a bheith ina mhodh úsáideach chun a thaispeáint go bhfuiltear ag comhlíonadh oibleagáidí slándála, i gcás go dtugtar le fios leis an deimhniú gur cuireadh rialuithe slándála sonraí faoi iniúchadh nó faoi athbhreithniú in aghaidh caighdeán aitheanta ag eagraíocht tríú páirtí a bhfuil dea-chlú uirthi. I gcomhthéacs na néalríomhaireachta, ba cheart do chustaiméirí a sheiceáil an féidir nó nach féidir le soláthraithe seirbhísí néalríomhaireachta cóip den deimhniú iniúchóireachta tríú páirtí sin a chur ar fáil agus dáta agus raon an deimhnithe a athbhreithniú.

I gcás go dtairgeann Soláthraithe Seirbhísí Néalríomhaireachta Clásail Samhla, is féidir gur leor tuarascáil iniúchóireachta ábhartha ó thríú páirtí a thabhairt in ionad ceart aonair chun iniúchadh. Is féidir gur míphraiticiúil ón taobh teicniúil de a bheidh iniúchtaí aonair ar shonraí a óstáiltear i dtimpeallachtaí freastalaí fhíorúlaithe ilpháirtí agus is amhlaidh dáiríre go méadóidh siad na rioscaí do na rialuithe slándála fisiciúla agus loighciúla líonra atá i bhfeidhm. Is é an rialaitheoir sonraí, áfach, atá freagrach as cinntiú go bhfuil sé/sí sásta leis na soláthairtí slándála atá déanta, agus as socrú conas is féidir é seo a thaispeáint mas gá é.