Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
5.tbl.3.árgangur 2013

Hlekkir

Heimasíða Deloitte

Tengiliðir

Jón Kristinn Ragnarsson
Sérfræðingur | ERS
jon.kristinn@deloitte.is
+ 354 866 9828

Úlfar Andri Jónasson
IT sérfræðingur | ERS
ulfar@deloitte.is
+ 354 866 1516

Kæri viðtakandi,

Áhættuþjónusta (ERS) er sérfræðihópur innan endurskoðunarsviðs Deloitte ehf. sem sérhæfir sig í innra eftirliti upplýsingakerfa, upplýsingaöryggi og endurskoðun upplýsingakerfa. Vírinn er gefinn út á tveggja vikna fresti og ætlaður m.a. stjórnendum, kerfisstjórum og almennum notendum upplýsingakerfa.

Gagnasölumenn eru stórtækari en fólk grunar

Upplýsingar um neytendur seldar dýrum dómi

Margir gera sér hugsanlega ekki grein fyrir að miklu magni upplýsinga er safnað um alla þá sem fara um Internetið nú til dags og einhverjir halda hugsanlega að með búsetu á Íslandi séu viðkomandi lausir við þennan vanda. Svo virðist ekki vera miðað við nýjustu fréttir, en nýleg grein sýnir að gögn um neytendur og notendur eru mikið notuð, meðal annars til að reyna að selja enn meira af vörum og þjónustu til neytenda. Ótrúlegustu aðferðir eru notaðir til að safna upplýsingum um fólk og síðan eru þessar upplýsingar settar saman með öðrum til að skapa heildstæða mynd af viðkomandi neytanda. Vandinn virðist vera að erfitt er að koma í veg fyrir þessa söfnun upplýsinga og mjög erfitt að segja til um hvernig þær eru notaðar. Engin ástæða er til að halda að þetta eigi ekki einnig við um tölvur sem eru tengdar netinu frá Íslandi, og/eða seljendur vöru og þjónustu á Íslandi.

Meira

Innsláttarveikleiki fyrir Android síma

Fimir fingur geta mögulega komist yfir upplýsingar úr læstum símum

Nýlega greindi Vírinn frá veikleika sem fundist hafði í iPhone símanum sem byggðist á „handlagni“ þess sem vildi komast í símann og þurfti að ýta á takka símans í sérstakri röð til að komast framhjá læsingu. Núna hefur álíka veikleiki komið fram fyrir Android símannog hefur til dæmis verið greindur á Galaxy Note II. Virkar þessi veikleiki þannig að farið er í gegnum

neyðarsímtalsmöguleikann og ef miðtakkanum er haldið inni ætti heimaskjár tækisins að birtast. Með hraða er þá hægt að ræsa það sem birtist snarlega á skjánum. Veikleikinn er þó takmarkaður að því leyti að læsingin kemur aftur upp, og er þess vegna ekki hægt að keyra forrit á símann. Það er hins vegar hægt að hringja í einstaklinga úr símanum í þeim tilvikum þegar flýtileiðir eru á heimaskjánum. Ekki er um stóran veikleika að ræða, en hugsanlega upphafið af fleiri álíka veikleikum.

Meira

Nýjar tegundir varna gegn óværu koma fram

Er hin sjálfstæða vörn að koma fram?

Seinni hluta árs 2012 kom fram óværa sem herjaði á Cisco símabúnað, og hefur, samkvæmt heimildum Vírsins, þessi tiltekni búnaður meðal annars verið notaður í Hvíta Húsinu og í flugvél forseta Bandaríkjanna. Óværan gerði óviðkomandi aðilum kleift að komast inn í símtöl, taka upp símtölin og svo framvegis. Nú hefur nokkrum vísindamönnum tekist, ekki einungis að koma með lausn á þessum vanda, heldur hugsanlega að koma með enn þróaðri leið til að verjast óværu en nokkru sinni áður. Rannsakendurnir hafa hannað kóða sem fer í og skannar viðkomandi tæki mjög hratt og í sífellu til að sjá hvort nokkuð óeðlilegt sé að gerast. Í hefðbundnum vírusvörnum þarf að koma upplýsingum til viðkomandi varnar til að hún þekki viðkomandi óværu. Í þessu tilviki fer vörnin að þekkja hegðun og afleiðingar óværu, og getur þannig unnið gegn henni. Vírinn fylgist spenntur með því hver þróunin verður í þessum málum.

Meira

Er IOS að deila meiri upplýsingum en Android?

Hinn sífelldi samanburður heldur áfram

Mikið er talað um hversu öruggir snjallsímarnir eru og hvort mögulegt sé að koma óværu í símana. Flestir eru þó sammála að helsti veikleiki upplýsingaöryggis sé notandi símans, og þá hafa rannsóknir sýnt að IOS, stýrikerfi iPhone og iPad, getur verið hættulegri en Android stýrikerfið. Nýleg rannsókn sem gerð var á 50 vinsælustu forritum sem sótt hafa verið á hvora tegund tækis sýnir að í langflestum tilvikum voru IOS forritin að óska eftir mun meiri aðgangi að upplýsingum á símanum en gert var í tilviki Android. Af þeim forritum sem skoðuð voru á IOS sendu 100% af þeim ódulrituð gögn, en það gerðu einungis 92% af Android forritum. Yfir helmingur af forritum á IOS fengu aðgang að tengiliðum í símanum. Í tilviki Android síma spyr forrit um leyfi að viðkomandi gögnum við uppsetningu og svo við uppfærslur, en þannig er ekki farið með IOS, og samkvæmt rannsókninni er mögulegt að breyta réttindum forrits eftir að það hefur verið sett upp. Þar getur vissulega leynst hætta sem notendur þurfa að vita af.

Meira

Endilega hafið samband við undirritaða (tengiliðir hér til hliðar) ef þið hafið spurningar eða frekari áhuga á efninu.

Viðtakendur eru hvattir til að áframsenda Vírinn á áhugasama

Kveðja,

Áhættuþjónusta Deloitte / Ritnefnd

Smáratorg 3
201 Kópavogur
Iceland

© 2013 Deloitte ehf.

Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see **www.deloitte.com/about** for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte RSS feeds
Afskráning