Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
8.tbl.3.árgangur 2013

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.

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

Enn eitt stórt innbrot í tölvukerfi samfélagssíðu

Að þessu sinni var brotist inn hjá LivingSocial

LivingSocial er tilboðssíða þar sem ný tilboð, sem tengjast helst ákveðnum borgum, á gistingu, málsverðum, sýningum og þess háttar, koma inn reglulega. Nýlega var brotist inn í netkerfi síðunnar og lykilorðum 50 milljón notenda stolið, auk þess sem komist var yfir nöfn, tölvupóstföng og, í sumum tilfellum, fæðingardag viðkomandi. Tekið hefur verið fram að lykilorðin hafi verið dulrituð með SHA1 (*hash*) dulritun og 40-bita söltun (Þetta þýðir að lykilorð notenda er fyrst sett í gegnum algóritma sem breytir lykilorðunum í einstakan gagnastreng, og svo tekur söltunin við – lengir gagnastrenginn enn meir og eykur flækjustigið). Það getur þannig orðið erfitt að brjóta upp þessi lykilorð, en Livingsocial hafa þó aukið öryggisstog sitt eftir innbrotið og notast nú við betri dulritun en áður (*bcrypt*). Notendum er þó vitanlega ráðlagt að breyta lykilorðum á síðunni, öllum síðum þar sem sama lykilorð er notað, og að vera á varðbergi gagnavart tilraunum til svindls með þeim upplýsingum sem stolið var.

Meira

Twitter aðgangar fréttaveita geta verið verðmætir

Síðast var Twitter aðgangi AP stolið, nú The Guardian

Nýlega var Twitter aðgangi The Associated Press (*AP*) stolið, og hann notaður í vafasömum tilgangi. Var meðal annars reynt að senda út fréttir um að sprenging hafi verið í Hvíta Húsinu, og að forseti Bandaríkjanna væri særður. Tilgangurinn virðist þannig ekki vera sá sami og stundum

hefur verið með stuld á Twitter aðgangi, s.s. til að birta hatursskilaboð heldur var þetta tilraun til að blekkja notandann. Fréttaveitur geta verið eftirsóknarverðar vegna fjölda þeirra sem fylgjast með þeim. Núna hefur 11 Twitter aðgöngum The Guardian verið stolið, og virðist sem um sömu aðila sé að ræða en í þetta sinn nota þeir aðgangana í áróðursskyni. Aðilar sem kenna sig við Syrian Electronic Army (*SEA*) virðast hafa aðgangana í sínum höndum, og birta þar tilkynningar. Samkvæmt SEA var ráðist á þessar veitur vegna þess að þær hafi farið hörðum orðum um Sýrland, og er hér um að ræða aðgerðir til að koma „sannleikanum“ á framfæri.

Meira

Munu stjórnendur hætta að greiða fyrir vinnutæki?

Nýleg rannsókn Gartner bendir til yfirvofandi breytinga

Mikið hefur verið fjallað um hvort starfsmenn eigi að fá að koma með og nota eigin tæki til vinnu, hið svokallað BYOD-vandamál (*bring your own device*), eða hvort einungis ætti að notast við tæki sem keypt eru og leyfð af yfirmönnum fyrirtækja. Margar spurningar eru tengdar þessu vandamáli og eru miklar spurningar um öryggi. Spurt er hvort yfirmaður getur krafist aukins öryggis á tæki sem notandinn á sjálfur og hvort það sem starfsmaðurinn gerir með tækið utan vinnu getur sett vinnugögn í hættu? Nýleg rannsókn Gartner greinir frá að fyrir árið 2017 muni meirihluti fyrirtækja hafa tekið þá stefnu að leyfa starfsmönnum að koma með eigin tæki til vinnu, en að stjórnendur muni taka þátt í kostnaði vegna notkunar og að sjálfsögðu að setja reglur um notkun tækjanna. Margir virðast hafa hingað til veigrað sér við að setja reglur um notkun slíkra tækja í eigu starfsmanna, en samkvæmt Gartner er þetta allt að koma.

Meira

Google og fleiri borga fyrir fundna veikleika

Væri hægt að nota sama fyrirkomulagi annars staðar?

Google tilkynntu nýlega að þeir hefðu borgað sérfræðiaðila á sviði tölvurannsókna í Bandaríkjunum rúmlega 30 þúsund dollara fyrir veikleika sem viðkomandi aðili fann upp á eigin spýtur og tilkynnti um í Chrome vafranum. Nokkur fyrirtæki hafa greitt sambærilegar greiðslur til slíkra aðila, t.d. Google og Firefox, en flest fyrirtæki birta þó ekki hversu mikið er greitt eða hver viðtakandinn er. Hér er um að ræða mjög áhugavert hvatningarkerfi til tölvugrúskara sem hefur skilað því að mjög margir veikleikar hafa fundist og verið lagaðir áður en hægt var að misnota þá. Þá hafa einnig verið haldnar keppnir þar sem leitað er að veikleikum í ákveðnum kerfum og hefur það einnig skilað góðum árangri. Veikleikar í vöfrum geta vissulega haft mikil áhrif ef þeir eru misnotaðir, en það er ljóst að mörg fleiri kerfi þurfa á slíkum hvatningarkerfum að halda til að finna veikleika. Mætti þá hugsanlega einnig nota sama kerfi til að finna veikleika í ríkjum?

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

Deloitte RSS feeds
Afskráning