Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
4.tbl.3.árgangur 2013

Kæri viðtakandi,

Áhættuþjónusta (ERS) er sérfræðihópur innan 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.

Endurnýjun á eldri óværu

Ef eitthvað virkar ekki, þá er það aðlagað – líka hjá glæpamönnum

Glæpamenn halda áfram að aðlaga sig breyttum aðstæðum í heiminum og í breyttu er mikilvægt að finna sína hillu. Nýlega hefur komið fram að glæpamenn eru farnir að endurnota gamlar óværur og orma til nýrra nota. Þau dæmi sem hafa verið tekin eru meðal annars „*Citadel*“ ormurinn, sem hefur verið einn skæðasti ormurinn sem eltist við bankaupplýsingar. Þessum ormi hefur nú verið breytt þannig að nú eltist hann við upplýsingar, hvort sem er leynilegar stjórnsýsluupplýsingar eða mikilvægar viðskiptaupplýsingar, og eru þær svo seldar hæstbjóðanda. Samkvæmt fréttum er þessi iðja ábótasamari en að eltast við bankaupplýsingar, sem bendir þá til hvoru tveggja að erfiðara sé orðið að þéna með stolnum bankaupplýsingum, en einnig að stór markaður sé fyrir stolnar upplýsingar. Vírinn ítrekar nú sem fyrr hversu mikilvægt það er að verja vel þær upplýsingar sem við viljum ekki að lendi í höndum ókunnugra.

Meira

Enn um veikleika í iPhone

iPhone símar virðast ekki jafn öruggir og margir vilja halda fram

Nýlega hafa komið fram veikleikar í iPhone sem hafa opnað fyrir aðgang að upplýsingum í símanum þótt hann sé læstur með talnakóða. Er þetta gert með því að fylgja ákveðinni ásláttarsamsetningu auk þess sem notast er við möguleika þess að hringja neyðarsímtöl án þess að aflæsa símanum. Nú hefur annar veikleiki komið fram sem virðist gera kleift að komast enn lengra. Þessi veikleiki opnar á möguleika á að tengja læstan síma við tölvu og ná upplýsingum af símanum án þess að aflæsa honum, en rétt er að taka fram að það krefst þess þá vitanlega að hafa símann í fórum sínum. Þótt það minnki hugsanlega alvarleika veikleikans er samt um alvarlegan hlut að ræða á meðan fólk heldur áfram að týna símum sínum. Apple hefur greint frá að

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

þeir muni bregðast við þessum veikleika fljótlega.

Meira

DDoS árás notuð til að hylma yfir innbrot á bankareikninga í BNA

Vandamál og óeðlegir hlutir eru oft vísbending um að eitthvað sé gruggugt
Á aðfangadag 2012 átti sér stað stór dreifð árás (DDoS) á banka nokkurn í Bandaríkjunum. Þegar róaðist kom hins vegar í ljós að þessi stóra árás hafði verið framkvæmd til að dylja smærra innbrot sem átti sér stað þar sem hundruðum þúsunda dollara var stolið af reikningum fyrirtækja sem voru í viðskiptum við bankann. Þau fyrirtæki hafa greint frá að fyrr þann dag höfðu verið vandamál við að komast inn á netbanka fyrirtækisins, og að síðan hafi verið óaðgengileg. Nú hefur hins vegar verið skýrt frá að þá þegar hafi tölvuþrjótarnir verið komnir með aðgang að tölvum fyrirtæksins, og þegar kom að því að stela fjármunum af reikningum var sett af stað stór dreifð árás til að dylja það sem fór fram. Peningunum var svo dreift á marga aðila sem flestir vissu ekki að verið væri að nota þá í peningaþvott, og höfðu það starf að áframsenda fjármuni á aðra reikninga gegn því að halda smávægilegum hluta eftir fyrir sjálfa sig.

Meira

Síða NBC deilir út óværu

Mikilvægt er að muna að það er ekki nauðsynlegt að smella lengur
Nýlega fór óværa sem komið hafði verið fyrir á síðu NBC fjölmiðlafyrirtækisins í Bandaríkjunum að reyna að dreifa óværu til allra sem rötuðu inn á síðuna. Var það gert með innsetningu (*iframe*) á síðunni sem reyndi að koma sýkingunni inn í flestar af þeim tölvum sem komu á síðuna. Þá náðist einnig að komast yfir nokkrar af undirsíðum, svo sem síðu Jay Leno og Jimmy Fallon, og reyndu þær einnig að dreifa sömu óværu. Það sem reynt var að dreifa var meðal annars óværa af „*Citadel*“ ættinni sem talað er um annars staðar í þessum Vír, og er tilgangur þess að eltast við bankaupplýsingar. Síðan virðist einungis hafa verið sýkt í stuttan tíma, en þó er víst að þegar hefur verið unninn mikill álitsskaði.

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