Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
9.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

Áherslur tölvuinnbrota að breytast?

Betra að láta skotmörkin koma til vopnsins

Ef reyna á að brjótast inn í tölvukerfi fyrirtækis myndu margir segja að besta leiðin væri að beina spjótum sínum að fyrirtækinu sjálfu og reyna þannig að finna glufur á vörnum þess. Í nýlegum dæmum virðist öðrum aðferðum vera beitt. Notuð hefur verið aðferð sem hægt er að kalla „vatnsbólsaðferðin“ en í stað þess að finna leiðir til að brjótast inn í tölvukerfi ákveðins fyrirtækis, sem getur hugsanlega verið með hátt öryggisstig og miklar varnir, er frekar reynt að komast yfir netsíður sem starfsmenn þessa fyrirtækis eru líklegir að heimsækja. Á þann hátt er hægt að sýkja tölvur viðkomandi starfsmanna með tölvuóværu og komast þannig inn fyrir netkerfi fyrirtækjanna sem þeir starfa hjá. Í nýlegu tilviki var vefsíða iðnaðarráðuneytis Bandaríkjanna sýkt og þá sérstaklega síður sem höfðu upplýsingar um kjarnorkumál. Er reiknað með að tilgangur sýkingarinnar hafi verið að reyna að komast inn í fyrirtæki sem eru líklegir notendur þessara síðna. Ljóst er að öryggisstjórar og -sérfræðingar þurfa að hugsa fyrir ýmsu til að halda netkerfum fyrirtækja öruggum.

Meira

Peningar vaxa ekki á trjánum á netinu

Erfiðar aðstæður efnaminni aðila notaðar til peningaþvættis

Nýlega var meira en einni milljón Bandaríkjadala stolið frá sjúkrahúsi í Washington í Bandaríkjunum. Var þetta gert með því að brjótast inn í tölvukerfið, komast yfir aðgang að launakerfi sjúkrahússins og voru millifærðir fjármunir á 96 mismunandi bankareikninga víðsvegar um Bandaríkin. Eigendur

þessara bankareikninga höfðu margir svarað auglýsingum með gylliboðum og voru alls kyns blekkingar notaðar til að fá þessa aðila til að gefa upp bankareikninga sína.. Í erfiðu árferði, eins og því sem hefur verið síðustu misseri í Bandaríkjunum getur verið heillandi að auka innkomu heimilisins með litlu vinnuframlagi. Allir þessir aðilar sögðu svipaða sögu, þ.e. að „starf“ þeirra átti að felast í að taka við fjármunum og millifæra áfram á erlenda reikninga, en þeir áttu að halda ákveðnu hlutfalli af greiðslunni eftir fyrir sig. Í þessu tilviki átti að áframsenda fjármuni til Rússlands og Úkraínu. Erfitt getur verið fyrir yfirvöld að elta fjármuni milli landa, en ljóst er að það fyrsta sem yfirvöld gera er að frysta þá litlu fjármuni sem „starfsmennirnir“ áttu að fá fyrir sitt viðvik.Seinna má ætla að komi lögsóknir á hendur þeim vegna aðildar að glæpastarfsemi.

Meira

Er aðskilnaður á milli vefkerfa leiðin til að tryggja öryggi?

Auknar hættur við hýsingu ef margir eru í sömu hýsingunni

Margar nútíma vefsíður og þjónustur eru ekki hýstar einar og sér á vefþjóni, heldur deila þeim þjónum með mörgum öðrum vefsíðum/þjónustum. Í nýlegri árás á nokkrar ísraelskar vefsíður kom í ljós veikleiki sem mörgum hefur hugsanlega ekki verið ljós hingað til, það er að vefsíða eða þjónusta sem ekki er fyllilega varin fyrir utanaðkomandi árásum getur opnað fyrir greiða leið að vefþjóninum sjálfum, sem getur þannig veitt aðgengi að öðrum vefsíðum og þjónustum sem sjálfar hafa verið betur varðar og uppfærðar. Þetta þýðir að öryggi vefsvæða og kerfa byggjast ekki eingöngu á hversu vel umráðamaður vefsvæðisins stendur sig í öryggismálum og uppfærslum, heldur þarf einnig að treysta á að þeir sem sjá um vefþjóna sem hýsir þær vefsíður eða þjónustur séu einnig að standa sig. Ýmsar aðferðir standa til boða, og er öllum lesendum Vírsins ráðlagt að kanna hvernig ykkar hýsingaraðili tryggir að sýkingar og þrjótar komist ekki óhindrað frá hýsingarnágrönnum ykkar.

Meira

Nettengdur hlutur eru hlutur í hættu

Sjúkratól eru ekki undanskilin almennri hættu

Vírinn hefur áður fjallað um hættuna sem getur fylgt því að vélbúnaður og önnur tæki séu tengd við Internetið, og að mikilvægt sé að taka öryggið með í reikninginn. Umræðan er ekki síst mikilvæg þegar kemur að umræðu um þau tæki sem notuð eru á sjúkrahúsum af heilbrigðisstarfsfólki, en ekki síður þegar kemur að lækningatækjunum, svo sem insúlíndælum eða gangráðum, sem eru í meira mæli orðin nettengd. Með aukinni kröfu um að allt sé aðgengilegt og sítengt getur það opnað fyrir veikleika af ýmsu tagi og þegar tækin eru ekki þróuð með netöryggi í huga getur orðið voðinn vís. Í einhverjum tilfellum er reynt að fylla upp í mögulegar öryggisglufur varðandi netöryggi eftir á með misjöfnum árangri. Þrátt fyrir að erfitt sé að hugsa sér að nokkur myndi reyna að skemma eða hafa áhrif á lækningatæki er einnig ljóst að hugur manna er seint fullkannaður. Þá er einnig mikilvægt að hafa hugann við að óviljaverk geta

einnig haft mikil áhrif í sítengdu umhverfi

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