Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
7.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.

Samstarf Deloitte og RM Studio

Tveir sterkir aðilar taka höndum saman um mikilvægt kerfi

Ritað hefur verið undir samstarfssamning milli Deloitte og Stika sem felur í sér að Deloitte mun verða umboðsaðili fyrir Risk Management Studio (RM Studio). RM Studio er áhættustjórnarhugbúnaður sem þróaður hefur verið af Stika og er notaður um allan heim. Samstarfið felur í sér að Deloitte mun taka að sér ráðgjöf vegna RM Studio og gerir kleift að ná til nýrra markaða og efla RM Studio um leið.

Meira

Strax komin óværa vegna árásarinnar í Boston

Nokkrum klukkutímum eftir sprengingarnar var óværan komin af stað

Líkt og Vírinn hefur áður fjallað um nota tölvuþrjótar öll tækifæri sem gefast til að reyna að blekkja tölvunotendur og koma óværu í tölvur þeirra. Eru nú þegar farnar að berast fréttir um að póstar hafi verið sendir út þar sem lofað er myndum af sprengingunum en þegar betur er að gáð kemur í ljós að um óværu er að ræða. Svipaðar tilraunir hafa einnig fundist á Facebook, þar sem reynt er að fá notendur til að smella á hlekki, annað hvort til stuðnings fórnarlömbum eða til að reyna að fá frekari upplýsingar um árásina. Vírinn minnir enn á mikilvægi þess að nálgast fréttir og upplýsingar einungis með viðurkenndum leiðum, og ekki taka gylliboðum sem fylgja því miður atburðum sem þessum. Mikilvægt er þá að kanna vel hvert hlekkir beina notendum og láta ekki forvitnina ráð för þegar smellt er á myndbönd.

Meira

Stórfelld árás á Wordpress síður í gangi undanfarið

Wordpress síður notaðar til að stækka og styrkja botnet

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

Wordpress er eitt stærsta ókeypis vefumsýslukerfi á netinu, en talið er að 17% síðna á netinu notist við Wordpress, og mjög auðvelt getur verið að setja upp slíkar síður. Þá er líka auðveldara en ella að notast aðeins við lágmarksöryggi. Nýlega fór Wordpress að bjóða upp á möguleika á tvöföldu innskráningaröryggi (*two-factor authentication*), og í framhaldi af því fór að bera á tilraunum til innbrota. Árásin er framkvæmd af stóru botneti (her af sýktum tölvum) og reynir að brjótast inn í gegnum *admin* notendur Wordpress síðunnar. Tilgangur með þessari árás virðist vera að byggja upp enn stærra botnet með því að komast yfir þessar síður, og þar með hugsanlega vefþjóna sem undir liggja. Lokatilgangur gæti síðan verið enn stærri árás, með enn meiri skaða.

Meira

Alltaf möguleiki á að uppfærslur valdi skaða

Ávallt mikilvægt að fara varlega – líka þegar kemur að uppfærslum

Nýlega sendi óværuvarnarfyrirtækið MalwareBytes frá sér uppfærslu á hugbúnaði sínum, en fyrirtækið hefur lengi verið í öryggisbransanum. Um var að ræða skilgreiningarskrá, sem á að segja hvaða skrár teljast vera óværa og hverjum eigi þá að reyna að eyða eða færa í sóttkví. Strax kom þó í ljós að ekki var allt með felldu, en þessi uppfærsla gerði það að verkum að ósmitaðar skrár voru sagðar smitaðar, og voru þess vegna gerðar óvirkar. Þetta voru hins vegar mikilvægar skrár fyrir keyrslu margra kerfa, og hafa margir notendur kvartað yfir að netþjónar hafi hreinlega ekki virkað eftir uppfærsluna.

MalwareBytes hefur viðurkennt að um mistök hafi verið að ræða og að þegar hafi verið brugðist við til að þetta komi ekki fyrir aftur. Það er hins vegar ljóst að í þessu hraða umhverfi þar sem nauðsynlegt er að bregðast við óværu sem allra fyrst geta mistök sem þessi auðveldlega komið fyrir. Erfiðara er hins vegar að vita hvað skuli til bragðs taka, enda er ljóst að uppfærslur öryggishugbúnaðar eru í flestum tilvikum bæði öruggar og bráðnauðsynlegar. Þetta er áhætta sem kerfisstjórar þurfa að hafa í huga, en þetta ítrekar enn nauðsyn á góðu og skilvirku afritunarferli.

Meira

Siðferði í viðskiptum er ekki útdautt

Ekki auðvelt að vera útgefandi skírteina á netinu

Moziilla, fyrirtækið að baki FireFox vafranum, íhugar nú að loka fyrir skírteinaútgefandann TeliaSonera. Áður hefur verið fjallað um skírteinaútgáfur í Vírnum, en slíkar útgáfur selja skírteini sem vottun um heilindi vefsíðna og þjónustu. Fyrir nokkrum misserum var brotist inn í nokkrar útgáfur á netinu og rafrænum skírteinum stolið, þannig að mögulegt er að glæpamenn geti blekkt netnotendur með notkun þessara skírteina. Netvafrinn treystir á slík skírteini til að vita að vefsíður séu þær sem þær segjast vera, en þegar skírteini eru misnotuð opnar það fyrir möguleika á blekkingum, til dæmis með svokölluðum *man-in-the-middle* blekkingum. Í þeim tilvikum hefur óprúttinn aðili komið sér á milli notenda og vefþjónustu, til dæmis til að reyna að fá viðkvæmar upplýsingar frá notandanum.

Ástæða þess að Mozilla íhugar að loka fyrir TeliaSonera er að upp hefur komið að

TeliaSonera hefur verið að selja skírteini til einræðisherra sem hafa stundað njósnir um íbúa ríkja sinna. Með slíkum skírteinum er mögulegt fyrir þessa einræðisherra að blekkja notendur, til dæmis með því að setja upp falskar Gmail eða Facebook síður – með skírteinum sem segja að síðurnar séu réttmætar, og komast þannig að viðkvæmum leyndarmálum. Ekki er fyllilega ljóst hvernig þetta endar, enda hefur TeliaSonera ekki brotið lög með athæfi sínu, en Mozilla virðist hafa víðtækan stuðning fyrir aðgerðum sínum.

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