Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
6.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

Stærsta tölvuárás sögunnar vegna mjög gamals galla?

Hversdagslegar stillingar geta haft mikið að segja

Undanfarið hafa verið áberandi í fréttamiðlum fréttir um það sem kallað hefur verið ein stærsta netárás sem framkvæmd hefur verið. Er þar átt við árásina sem framkvæmd var á SpamHaus, en það er fyrirtæki sem greinir uppruna ruslpósts og reynir að koma í veg fyrir dreifingu hans. Talað hefur verið um að árásin á SpamHaus hafi hægt á öllu Internetinu. Nú hefur komið í ljós að mjög gamall og algengur veikleiki í DNS netþjónum var notaður í þessari árás, (DNS þjónar sjá um að breyta „heimilisfangi“ síðu úr talnarunu í þær slóðir sem notendur þekkja), og hefði verið hægt að minnka umfang hennar umtalsvert með einföldum aðgerðum. Með veikleikanum er hægt að nota DNS þjóna til að magna upp umferð, og þannig valda því sem kallað hefur verið *„Árásin sem braut næstum Internetið“*. Minnir þetta enn á hversu mikilvægt er að fara yfir stillingarnar.

Meira

Evernote notað til að stjórna botnetum

Breyttar aðstæður krefjast frekari varna

Vírinn hefur fjallað um mörg af þeim botnetum (samansafn af sýktum tölvum) sem gerð hafa verið óvirk undanfarin misseri, meðal annars með samstarfi löggæsluaðila og stórra fyrirtækja. Microsoft hefur til að mynda verið öflugt í að fella botnet. Má þá telja að það sé eðlileg afleiðing af því að þeir sem reka botnet leiti á önnur mið til að valda smiti, og hafa hinar ýmsu skýgeymslur komið sterkar inn þar. Komið hefur í ljós að stjórnþjónar botneta, en það eru

þeir vefþjónar sem senda skipanir til sýktra tölva og taka jafnvel við stolnu efni, eru í auknum mæli hýstir í tölvuskýjum. Hefur þá verið talað um Dropbox, Box.com og Evernote. Þetta er gert til að komast hjá vörnum. Umsjónarmenn tölvukerfa geta lokað fyrir aðgang að þekktum sýktum þjónum, en oft er síður lokað fyrir þjónustur eins og Dropbox og Evernote. Þannig er hægt að viðhalda sýkingu, jafnvel á vel vernduðu neti.

Meira

Leynist gull í ruslinu þínu?

Mikilvægt að muna að farga viðkvæmum upplýsingum á öruggan máta
Gögn sem hefur verið hent í ruslið hjá fyrirtækinu þínu geta verið verðmæt fyrir óprúttna aðila sem vilja komast yfir viðkvæmar upplýsingar. Eru þar á meðal skjöl og önnur gögn sem ekkert er alltaf ljóst að geti talist viðkvæm. Dæmi um slíkt eruskjöl sem hafa merki (e.logo) fyrirtækis en þau er hægt að nota til að falsa skjöl, og ef óprúttnir aðilar komast yfir skjöl með undirskrift er hægt að falsa skjöl á trúverðugan hátt.. Færanlegir miðlar eins og USB kubbar og geisladiskar ættu aldrei að fara í ruslið án þess að öruggt sé að engin gögn séu á þeim. Handbækur sem innihalda viðkvæmar upplýsingar, jafnvel þótt þær séu úreltar, geta veitt möguleika á misbeitingu og svikum. Þess vegna er mikilvægt að hafa varann á sér þegar hent er í ruslið.

Meira

Nethernaður milli ríkja er í sífelldri þróun

Nýjar aðferðir vekja upp áhugaverðar spurningar
Baráttan milli Norður- og Suður Kóreu hefur harðnað undanfarið og hefur nethernaði vitanlega einnig verið beitt. Nýlega var greint frá í fréttum að tekist hafi að sýkja nokkrar tölvur í Suður Kóreu, meðal annars hjá tveimur bönkum og hjá **sjónvarpsstöð**. Skiptar skoðanir eru um þessa sýkingu, meðal annars um hversu þróuð hún var, en ljóst er að árásaraðferðin (e. attack vector) vekur upp áhugaverðar spurningar. Svo virðist sem sýkingunni hafi verið komið inn í netþjón sem sér um reglulega uppfærslu á nokkuð mörgum vélum og þannig hafi sýkingunni verið dreift á margar vélar. Oftast er um að ræða stærri net sem notast við slíkar vélar og getur þessi árásaraðferð þannig í raun einungis náð til stærri tölvuneta. Þetta vekur okkur til umhugsunar um hversu mikilvægt er að vernda vel þá vél (tölvu) sem hefur það hlutverk að deila uppfærslum á aðrar vélar. Ef ekki er vel að gáð getur hér komið fram alvarlegur veikleiki í vörnum fyrirtækja.

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,

Smáratorg 3
201 Kópavogur
Iceland

Deloitte RSS feeds
Afskráning