Deloitte.

Iceland
Upplýsingaöryggi

Vírinn
10.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.

Hlekkir

Heimasíða Deloitte

Tengiliðir

Jón Kristinn Ragnarsson
Sérfræðingur | ERS
jon.kristinn@deloitte.is
+ 354 580 3110

Úlfar Andri Jónasson
IT sérfræðingur | ERS
ulfar@deloitte.is
+ 354 866 1516

Fyrirtæki keppast við að taka upp tveggja þátta auðkenningu

Er hugsanlega um falskt öryggi að ræða?

Fyrstu viðbrögð margra tæknifyrirtækja (Twitter, Yahoo, WordPress, og fleiri) eftir innbrot í upplýsingakerfi þeirra er að taka upp hina svokölluðu tveggja þátta auðkenningu (*e. Two factor authentication*), þar sem ekki er nægilegt að notast eingöngu við lykilorð til að fá aðgang að upplýsingakerfum þeirra heldur þarf að auki annan og aðskilinn þátt, til dæmis SMS, fyrir notenda til að auðkenna sig. Þó að vissulega sé gott þegar fyrirtæki færa sig í átt að auknu öryggi getur verið um falskt öryggi að ræða. Nú þegar hafa tölvuþrjótar hannað óværu í tengslum við þetta þar sem tveir og jafnvel fleiri þættir eru vaktaðir af tölvuþrjótunum, til dæmis að sími sé hleraður eftir SMS skeyti sem sent er til auðkenningar en notandinn tekur ekki eftir neinu. Þá er það einnig þannig að sum fyrirtæki setja tveggja þátta auðkenningu ekki sem skyldu heldur sem val (*e. opt-in*) þannig að notandinn þarf í raun að velja að hann vilji aukið öryggi (og þannig aukið flækjustig fyrir sig), en margir notendur eru ekki til í það. Þannig að möguleiki á auknu öryggi tryggir ekki hærra öryggisstig. Þó er mikilvægt að hafa möguleikann á auknu öryggi.

Meira

Tilraunir til peningaþvættis í gegnum hótel

Mikið ber á tilteknum tegundum af svindlpósti

Undanfarið hefur nokkuð borið á svindlpósti þar sem sendandi óskar eftir að fá að bóka hótelherbergi á hóteli viðtakandans. Flestir myndu væntanlega hugsa að um rangan viðtakanda væri að ræða og henda bréfinu, nema einmitt starfsmenn hótela og gistihúsa. Þegar nánar er að gáð kemur hins vegar fram að um svindl er að ræða sem fer þannig fram að ef viðtakandi svindlpóstsins svarar póstinum og sýnir áhuga fær hann sendan bókunarpóst með stolnum greiðslukortaupplýsingum, auk þess sem

óskað er eftir að tekið sé framyfir á kortinu og mismunurinn sendur á starfsmann ferðaskrifstofu í gegnum Western Union. Ýmsar ástæður eru gefnar fyrir því að greiðsla til starfsmannsins þarf að fara þar í gegn. Þegar greiðslan hefur verið afgreidd er hætt við pöntunina, en þá hafa peningarnar skilað sér tandurhreinir í gegnum WU og til þeirra sem ætla sér að nota þá. Talið er að póstar sem þessir séu í flestum tilvikum sendir á upplýsingapóstföng, svo sem póstföng með „info“ forskeyti, og eru starfsmenn hótela og gistiheimila hvattir til að hafa varann á nú þegar straumur ferðamanna fer að aukast.

Meira

Takmarkanir frekar í hugbúnaði en vélbúnaði

Hagræðing í kerfi myndavélar eykur notkunarmöguleika hennar gífurlega
Komið hefur í ljós að mikið af rafmagnstækjum virðast vera takmörkuð af hálfu framleiðenda til þess eins að réttlæta að dýrari (og fleiri) hlutir séu keyptir. Nú hefur komið í ljós að Canon 50D myndavél frá árinu 2008,sem á samkvæmt framleiðslulýsingu ekki að hafa myndbandsupptökumöguleika, hefur þann möguleika sannarlega, og virkar mjög vel sem slík. Bendir þetta til þess að oft sé sami vélbúnaður notaður á milli véla, en takmarkanir séu frekar í hugbúnaðinum. Þetta hefur þá augljósa samsvörun við önnur tæki og tól tengd upplýsingatæknimálum og sýnir okkar að „fiktið“ borgar sig stundum, alla vega þegar afleiðingar þess eru notaðar til góðs. Fjölmörg dæmi úr Vírnum sýna hins vegar að slíkt „fikt“ er stundum og hugsanlega oftar notað til illra verka.

Meira

Ungir sem aldnir leita að göllum í kerfum

Á aldurstakmörkun rétt á sér í kóðarýni?
Í nýlegum Vír var fjallað um að tæknifyrirtæki væru farin að greiða notendum og rannsakendum þóknun fyrir að finna og benda á óþekkta galla í hugbúnaði sínum. Dæmi sem hafa verið tekin um slíkt eru til dæmis Google og Firefox. Nýlega fann ungur drengur í Þýskalandi galla sem tengist XSS (*e, cross site scripting* – galli í vefkerfi) hjá PayPal. Hafði þessi sami drengur áður fundið galla hjá Microsoft og Firefox, en þegar átti að greiða honum þóknun fyrir að finna gallann hjá Paypal reyndi tæknifyrirtækið að neita honum um greiðslu sökum þess að strákurinn var bara 17 ára gamall og var vísað í reglur PayPal um að viðkomandi væri of ungur til að fá greitt fyrir uppgötvunina.. Þrátt fyrir að PayPal hafi að lokum samþykkt að viðkomandi ætti að fá greiðsluna og muni endurskoða reglur sínar veltir þetta þó upp áhugaverðri spurningu hvort aldurstakmarkanir eigi nokkurn tíma rétt á sér í slíkum málum? Nú þegar krakkar niður í mjög ungan aldur eru farin að læra forritun og framfarir eru gífurlegar milli kynslóða er ljóst að aldur segir ekkert um hæfni til að greina kóða eða finna öryggisgalla.

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