Mikilvægi þess að setja netöryggi í forgang

Stella Thors,
sérfræðingur í
áhættugreiningu

Hér á landi hefur verið talað um tölvuárásir í mörg ár og hingað til höfum við ef til vill einungis tengt þær við bíómyndir enda hefur Ísland ekki orðið fyrir mörgum slíkum árásum. Frasar á borð við: „Þökk sé íslenskri tungu þá er Ísland ekki skotmark," hafa oft heyrst en miðað við þá tækniþróun sem orðið hefur við sjálfvirkar þýðingar tungumála má telja líklegt að ekki verði hægt að nota þessa afsökun mikið lengur. Eftir því sem fyrirtæki færa sig meira yfir í að vista og meðhöndla gögn stafrænt hafa líkurnar á netárásum aukist. Tíðni netárása hefur verið stigvaxandi undanfarin ár og hefur viðbúnaður fyrirtækja gagnvart slíkum árásum því aldrei verið jafn mikilvægur og hann er í dag. Það hefur haft þau áhrif að netógnir og varnir gegn þeim hafa færst ofar á forgangslista stjórnenda. Mikilvægt er að þessum málum sé sinnt af krafti og þess gætt að fræðslan nái ekki einungis til stjórnanda heldur til allra starfsmanna fyrirtækisins. Hægt er að kaupa allar öflugustu netvarnirnar og innleiða þær hjá fyrirtækinu en hafa verður í huga að það verður aldrei öruggara en veikasti hlekkurinn, sem í öllum tilvikum er starfsfólkið. Þann hlekk munu óprúttnir aðilar reyna að brjóta, því er mjög mikilvægt að starfsfólkið sé meðvitað um þær netógnir sem til staðar eru og fái fræðslu við hæfi.

Viðskipti yfir Internetið

Flest öll bankaviðskipti í dag eiga sér stað yfir net og fyrirséð að þau aukist jafnt og þétt í náinni framtíð. Það hefur jafnframt í för með sér að umfang rafrænna gagna eykst sífellt hjá fjármálafyrirtækjum. Fjármálafyrirtæki búa yfir viðkvæmum gögnum um einstaklinga og fyrirtæki, því hafa sjónir tölvuglæpamanna í auknu mæli beinst að slíkum fyrirtækjum. Þannig virðist hafa orðið 29% aukningin á árásum á fjármálafyrirtæki milli áranna 2015 og 2016[1] og á sú tala eflaust bara eftir að hækka. Mikilvægt er að vernda gögn fyrirtækja til að reyna að lágmarka líkurnar á því að gögn leki ef til árásar kemur, hvort sem hún er á ábyrgð utanaðkomandi aðila eða jafnvel einhvers innanhús. Eitt af því sem mikilvægt er að gera er að stýra aðgangi að gögnum og hafa mörg fyrirtæki tekið upp þá stefnu að starfsfólk hafi einungis aðgang að þeim gögnum sem það þarf til að geta sinnt í sínu starfi. Styrking varna gegn netógnum og gagnastuldi sem kemur „innanfrá" hefur að vissu leyti verið vanræktur af stjórnendum en meiri áhersla verið lögð á að verjast „utan að komandi" ógnum.

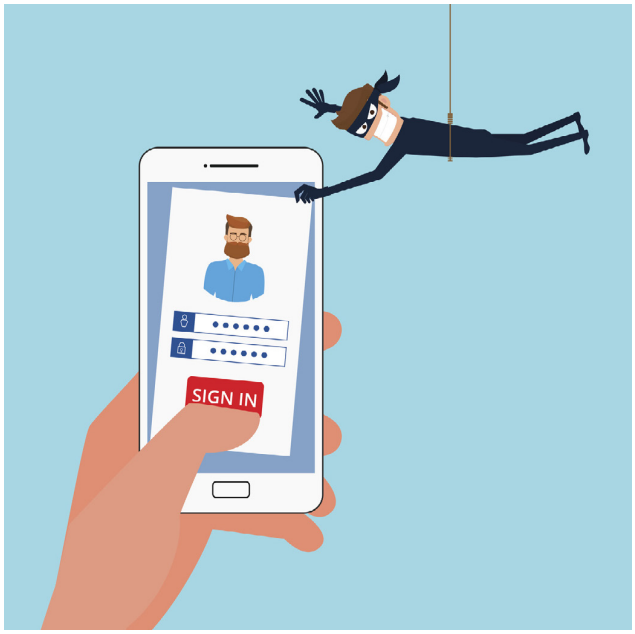
Mikilvægt er að þekkja helstu áhætturnar, kynna þær vel fyrir starfsfólkinu og þar með draga úr líkum á því að fyrirtækið eða stofnunin verði fyrir barðinu á óprúttnum aðilum. Fræðsla um varnir, viðbúnaður og æfingar vegna netógna ættu að vera jafn sjálfsagður hlutur og aðrar öryggisráðstafanir fyrirtækja.

Hvað ber að varast?

Gerandinn er minna sýnilegur en í öðrum glæpum þar sem netárásir eiga sér alltaf stað yfir Internet og glæpamaðurinn er oftast í öðru landi. Tölvuárásir krefjast alla jafna mikillar tækniþekkingar en þó eru til aðilar sem selja lausnir sem aðrir með minni tæknikunnáttu nýta sér, t.d. er hægt að kaupa hugbúnað sem framkvæmir árás á þriðja aðila eða einfaldlega kaupa þá „þjónustu" beint af óprúttnum aðilum. Kaup og sala stolinna gagna hefur jafnframt færst í aukana, m.a. kortaupplýsingar einstaklinga eða aðgangsupplýsingar þeirra að þjónustu- og fjármálalausnum. Þegar talað er um netógnir eða netárásir eru eftirfarandi tegundir árása oftast nefndar:

Gagnagíslatökur (e. Ransomware)
Gengur út á að hneppa gögn einstaklinga eða fyrirtækja í gíslingu með því að dulrita þau og krefjast síðan lausnargjalds vilji notandinn fá gögnin sín aftur. Tíðni slíkra árása á heimsvísu hefur aukist jafnt og þétt.

[1] http://www.darkreading.com/endpoint/financial-services-sector-the--1-target-of-cybercriminals/d/d-id/1328775



Vefveiðar (e. Phishing)
Gengur út á það að veiða notandann í gildru, t.d. með því að senda tölvupóst með hlekk eða viðhengi sem keyrir spilliforrit á vélinni eða vísar notandanum á óörugga vefsíðu. Falli notandinn í þá gildru er sendandi tölvupóstsins líklegast kominn með meiri aðgang að gögnum notandans en hann ætti að hafa.

Milliliðurinn (e. Man in the middle)
Hér kemst óprúttinn aðili í þá aðstöðu að ná að hlera samskipti á milli tveggja tölva og breyta innihaldi samskiptanna. Þetta er eitthvað sem t.d. netverslanir þurfa að gæta að og því mikilvægt að samskipti verslunar og viðskiptavinar séu dulkóðuð (e. Encrypted).

Álagsárás (e. DDoS)
Markmið þessara árása er að lama vissa þjónustu með því að gera vél eða netauðlind ekki tiltæka fyrir fyrirhugaða notendur hennar.

Kennistuldur (e. Identity theft)
Færst hefur í aukana að verið sé að taka aðgang fólks inn á samfélagsmiðla í gíslingu. Hingað til hefur þetta verið meira til ama en tjóns þar sem notandinn þarf oft að leggja í töluverða fyrirhöfn að endurheimta aðganginn sinn. Með aukinni tengingu samfélagsmiðla við þjónustuveitendur og vefverslanir hefur slíkur kennistuldur leitt til meira tjóns en áður þar sem persónuupplýsingar og mögulega greiðslukortanúmer eru vistuð hjá fleiri aðilum. Fyrir nokkrum árum var talað um að það væru einkum bólugrafnir unglingar í skítugum kjallaraholum sem stunduðu slíka iðju en í dag er þetta iðnaður sem sérhæfir sig í að stela upplýsingum og selja manna í millum á netinu. Hver sem er getur svo fyrir lítinn pening keypt slíkar upplýsingar og notað til að versla á netinu eða til úttektar af bankareikningum.

Aukin krafa um öryggi

Með tilkomu PSDII[2], nýrrar tilskipunar ESB um greiðslu-þjónustu sem líklega verður innleidd í íslensk lög á næsta ári, mun sú krafa vera gerð að notandinn auðkenni sig með því að nota fjölþátta auðkenningu þegar verslað er á netinu. Það þýðir að nota þarf fleiri en eina aðferð til að auðkenna sig t.d. með lykilorði og kóða sem sendur er í símann. Með þessu er hægt að minnka líkurnar á því að óprúttinn aðili komist yfir aðgang notandans. Algengt er að notendur noti sama lykilorðið á allar þær vefsíður sem krefjast innskráningar. Þegar lykilorð eru endurnýtt skapast sú áhætta að ef lykilorði notandans er stolið, t.d. á Facebook, þá er sá aðili sem komst yfir lykilorðið einnig kominn með aðgang að fleiru, t.d. heimabanka notandans.

Þegar viðskipti fara fram yfir Internetið er mikilvægt að hafa varann á. Í netverslun þarf yfirleitt að gefa upp viðkvæmar fjárhagsupplýsingar líkt og greiðslukortanúmer auk CVV2 öryggisnúmers[3] og annarra viðkvæmra upplýsinga. Notendur þurfa að gæta vel að fjárhagsupplýsingum og vera nokkuð öruggir um að greiðslugátt sé traust. Til dæmis er hægt að skoða hvort vefslóð síðunnar byrji ekki örugglega á https en ekki http, þar sem að s-ið stendur fyrir „secure“ eða öruggt. Í dag eru flestir vafrar stilltir þannig að þeir vara notendur við ef samskipti við ákveðna vefsíðu eru ekki talin örugg og sumir vafrar birta einfaldlega ekki síður sem eru http. Í dag bjóða flestir bankar upp á smáskilaboð til viðskiptavinar í hvert skipti sem að kreditkort hans er notað á netinu. Með því að nýta sér þessa þjónustu getur viðskiptavinurinn tilkynnt til bankans og/eða lögreglu ef tilhæfulaus úttekt hefur átt sér stað. Að lokum er gott að hafa í huga að ef tilboð á netinu hljóma of vel til að vera sönn þá kunna þau að vera það og full ástæða til að hafa varann á.

Í júlí 2016 samþykkti Evrópusambandið nýja tilskipun

[2] PSDII (Payment Services Directive 2), tilskipun (ESB) 2015/2366, er önnur tilskipun Evrópusambandsins um greiðsluþjónustu og er hluti af víðtækri löggjöf innan EES um greiðslumarkaði.
[3] CVV2 (Card Verification Value 2) er þriggja stafa öryggisnúmer (security code) sem er áprentað við hlið undirskriftarreits á bakhlið kortsins. Algengt er að söluaðili biðji um þetta þriggja stafa öryggisnúmer kortsins þegar greiðsla er framkvæmd án þess að korti sé framvísað, t.d. þegar vara og/eða þjónusta er pöntuð á netinu, í gegnum síma eða í pósti.

um net- og upplýsingaöryggi[4] (NIS) sem gert er ráð fyrir að verði tekin inn í EES-samninginn og innleidd í íslensk lög. Tilskipuninni er ætlað að auka hæfni aðildarríkjanna til að samræma viðbrögð þeirra við alvarlegri netógn og bæta þekkingu á þessum mikilvægu málefnum. Netógnir ná oft þvert á landamæri og algengt er að ráðist sé á fleiri en eitt land í einu. Því er mikilvægt að aðildarríkin vinni saman í baráttunni gegn slíkri ógn. Mikil áhersla er á að rekstraraðilar mikilvægra innviða samfélagsins séu meðvitaðir um þá áhættu sem tengist rekstri þeirra, að þeir geri áhættumat, útbúi viðbúnaðaráætlun og hafi ferla sem taka á því hverjum skuli tilkynna netógn og/eða árás sem þeir verða varir við. Ekki eru til þær varnir sem koma í veg fyrir allar alvarlegar netárásir en með því að þekkja eigin veikleika og hafa æft viðbrögð við netógnum má lágmarka tjón vegna þeirra. Mikilvægt er að fyrirtæki setji sér stefnu um net- og upplýsingaöryggi, skilgreini stefnumótandi markmið ásamt stefnu og reglu um ráðstafanir. Á vef samgöngu- og sveitarstjórnarráðuneytisins[5] kemur fram að undirbúningur að innleiðingu tilskipunarinnar hér á landi sé hafinn. Því er mikilvægt að kynna sér hana.

Hvað getum við gert?

Mikill hraði er í tækniþróun í heiminum og ljóst að öryggismál munu alltaf vera á hælunum á þeirri þróun. Með tilkomu NIS og PSDII mun krafan um aukið öryggi tengt fjárhagsupplýsingum verða sett fram á staðlaðan hátt. Miklar líkur eru á því lykilorð eitt og sér muni víkja fyrir nýjum fjölþátta aðferðum til auðkenningar sem t.d. byggja á líftækni. Dæmi um slíka auðkenningu er raddgreining, augnskanni eða fingrafaraskanni. Mun það eflaust gleðja marga sem eiga erfitt með að muna mörg lykilorð. Gjarnan er talað um að góð auðkenning samanstandi af einhverju sem notandinn veit, hefur og gerir.

Stjórnendur þurfa að gæta þess að netöryggismál fái sama vægi og önnur öryggismál innan fyrirtækisins. Boðleiðir og viðbrögð starfsmanna sem varir verða við netógnir þurfa að vera einföld, skýr og markviss. Segja má að þjálfun starfsmanna sé mikilvægasti hlekkurinn í öryggi fyrirtækja. Starfsfólk þarf að þekkja ferla fyrirtækisins og kunna að bregðast rétt við, hvort sem er í vinnunni eða heima. Orðaforði og málvitund tölvuþrjóta hefur tekið töluverðum framförum með hjálp öflugari þýðingarvéla og við stefnum hraðbyri í að tíðni fórnarlamba vefveiða hérlendis verði sú sama og í nágrannalöndum okkar. Því er mikilvægt að vera samstíga í því að fræða stjórnendur og starfsfólk fyrirtækja. Öryggissérfræðingar hafa bent á að öflug öryggisvitund og aðgát starfsmanna sé í raun besta forvörn sem hægt er að fjárfesta í.

Eins og fram hefur komið er nokkuð ljóst að alvarlegar netárásir geta leitt til fjárhagslegs taps, alvarlegs rekstrarrofs og jafnvel eyðilagt orðspor þess fyrirtækisins sem fyrir þeim verður. Það er því ástæða til að skora á stjórnendur fyrirtækja að kynna sér þessi málefni vel og æfa vel hvernig þeirra fyrirtæki ætla sér að bregðast við slíkum árásum, t.d. með því að framkvæma áhættumat, útbúa viðbúnaðaráætlun og kynna vel fyrir starfsfólki sínu hvaða ferlar eru til staðar standi það frammi fyrir slíkum áskorunum.

[4] The Directive on security of network and information systems (NIS Directive)
[5] https://www.stjornarradid.is/verkefni/almannaoryggi/netoryggi/