CERT·IS

ÁRSYFIRLIT 2021

CERT-ÍS er deild innan Fjarskiptastofu.
Málefni netöryggis heyra undir ráðuneyti háskóla- iðnaðar og nýsköpunar (HVIN)

CERT·IS

ÁRSYFIRLIT 2021

EFNI

Ávarp sviðsstjóra

Þann 1. september 2020 voru lög um net- og upplýsingaöryggi mikilvægra innviða, hin svokallaða NIS löggjöf, innleidd á Íslandi. Við þau tímamót var hlutverk og skipulag netöryggissveitarinnar CERT-ÍS stóreflt og hefur hún stækkað samhliða auknum áherslum og ábyrgð.

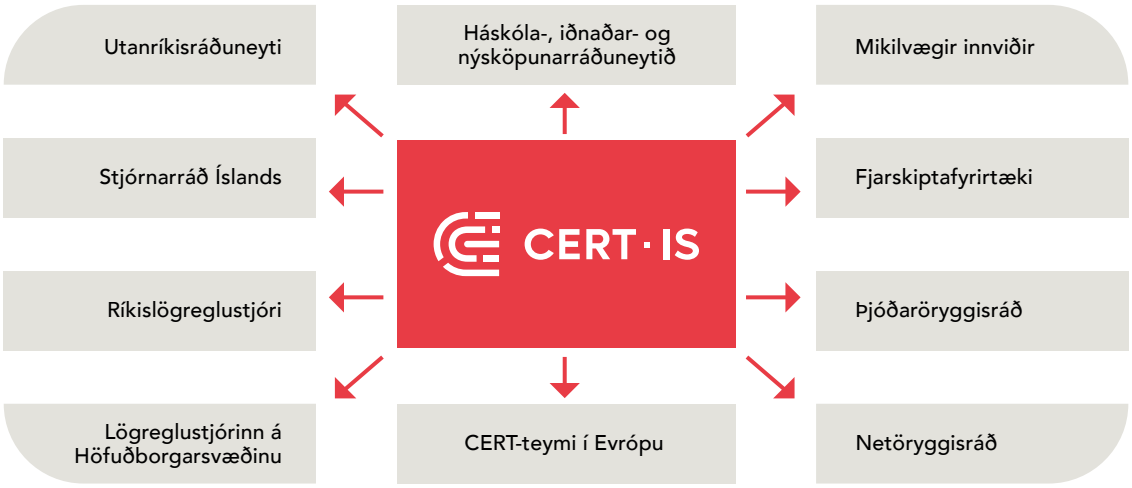
Í ljósi þess hve seint NIS lögin voru innleidd hérlendis má færa rök fyrir því að Íslendingar séu eftirbátar annarra þjóða hvað varðar uppbyggingu ráðstafana hins opinbera til að bregðast við netöryggisatvikum. Í mati Alþjóðafjarskiptasambandsins (ITU) eru Íslendingar í fararbroddi þjóða heims í notkun á net- og upplýsingatækni á meðan netöryggismálum sé ábótavant. Þessi staða getur verið ógn við almanna- og þjóðaröryggi og full ástæða til að bregðast við og stuðla sem fyrst að fullri uppbyggingu ráðstafana sem NIS löggjöfin gerir ráð fyrir.

Í nýjum stjórnarsáttmála er ein af stóru áskorunum að fara í stafrænar umbreytingar þar sem m.a. verður unnið markvisst að því að efla net- og fjarskiptaöryggi. Að mati CERT-ÍS er netöryggi meginforsenda stafrænnar umbreytingar. Sveitin hefur vel skilgreint samhæfingarhlutverk við miðlun upplýsinga og ráðgjafar í atvikameðhöndlun mikilvægra innviða ásamt því að viðhalda réttri ástandsvitund netöryggismála á landsvísu og miðla henni áfram innan íslenska netumdæmisins og til erlendra netöryggissveita.

Til að stuðla að öflugri atvikameðhöndlun hefur CERT-ÍS unnið að því undanfarið að koma á sviðshópum rekstraraðila nauðsynlegrar þjónustu. Nú hafa sviðshópar verið virkjaðir fyrir fjármálainnviði, fjarskiptainnviði og orkuinnviði. Virkjun sviðshópanna gerir ábyrgðaraðilum mikilvægra kerfisinnviða kleift að standa þéttar að netvörnum með meiri samvinnu.

Greina má mikla aukningu á öllum tegundum netárása og er það í samræmi við þróun mála hjá nágrannaþjóðum okkar. Aukningu árása má m.a. rekja til þess að tæknilegur þröskuldur sem þarf að yfirstíga til að geta framkvæmt fjölbreyttar tegundir árása hefur lækkað og það verður sífellt ódýrara að kaupa aðgengi að kerfum til að framkvæma slíkar árásir. Þar sem áður þurfti talsverða þekkingu á net- og tölvukerfum ásamt því að hafa beinan aðgang að búnaði til að framkvæma árásir, þá er í dag hægt að nýta sér lögleg og ólögleg tölvuský og kaupa sérhæfða þekkingu og þjónustu hjá öðrum glæpahópum.

Ábyrgðar- og rekstraraðilar mikilvægra innviða þekkja þessa þróun og má merkja aukinn slagkraft í umræðu um netöryggismál og eflingu almennrar netöryggismeðvitundar. Ánægjulegt er að merkja aukinn vilja til að ræða opinskátt um eðli og afleiðingar árása. Það er öllum til heilla að samnýta lærdóm af atvikum.



Til að uppfylla hlutverk CERT-ÍS, um að viðhalda ástandsvitund málaflokksins á Íslandi, ætlar CERT-ÍS að leggja áherslu á að vinna greinagóðar upplýsingar úr þeim vísum sem berast sveitinni og birta almenningi og þjónustuhópum, t.a.m. með skýrslu sem þessari. Áhersla verður lögð á að efla samstarf við erlendar netöryggissveitir sem er mikilvægt í ljósi þess að árásir í stafrænum heimi taka oftast ekki mið af hefðbundnum landamærum. Mikilvægt er að Ísland geti lagt lóð á vogarskálarnar í alþjóðlegu samstarfi.

Síðastliðið ár hefur verið viðburðaríkt fyrir CERT-ÍS. Sveitin hefur rúmlega tvöfaldast með aukinni ábyrgð og nýjum skilgreindum hlutverkum. En betur má ef duga skal. Gera má ráð fyrir að uppbygging netöryggissveitarinnar CERT-ÍS taki a.m.k. þrjú ár að því gefnu að skortur á björgum tefji ekki fyrir. Uppbygging netöryggissveitar er flókið ferli sem m.a. felur í sér innleiðingu og þróun regluverks, ráðningu og þjálfun starfsfólks, að koma upp vottaðri og öruggri starfsaðstöðu, útfæra verkferla og verklagsreglur, koma á skilgreindum þjónustuferlum og þjónustustigi alla daga ársins allan sólarhringinn, koma upp nauðsynlegum kerfum og tækjabúnaði, koma á og þróa alþjóðleg tengsl og byggja upp sviðshópa innanlands fyrir alla hópa mikilvægra innviða.

Afar mikilvægt er að stjórnvöld styðji þétt við bakið á uppbyggingu netöryggis-sveitarinnar þannig að Ísland nái að standa jafnfætis nágrannaþjóðum okkar sem fyrst á þessu mikilvæga sviði þannig að opinber markmið stjórnvalda náist hvað þetta varðar.

Virðingarfyllst.
Guðmundur Arnar Sigmundsson
Sviðsstjóri netöryggissveitarinnar CERT-ÍS

Árið 2021 í tölum

12 atvik

Upplýsingaöryggi

Aðgangur að upplýsingum eftir ólöglegum leiðum, gagnatap og gagnalekar.

22 atvik

Tiltækileiki

Kerfi og þjónusta ekki aðgengileg af ytri ásetningi, t.d. álagsárásir þegar þjónusta tölvukerfa er vísvitandi skert með yfirálagi.

446 atvik

Svindl

Netveiðar þar sem reynt er að komast yfir viðkæmar upplýsingar, s.s. kortanúmer eða lykilorð.

6 atvik

Níðingsefni

Einelti, áreitni og eltihrellni. Auk þess barnaníðsefni og upphafning ofbeldis.

23 atvik

Veikleikar

Veikleikar sem hægt er að nýta til að brjótast inn í eða hafa áhrif á tölvukerfi annarra.

16 atvik

Innbrot

Innbrot í tölvukerfi hjá heimanotendum, fyrirtækjum eða rekstraraðilum.

16 atvik

Spillikóði

Tölvuveirur og annar kóði sem notaður er til að eyðileggja eða ná stjórn á tölvukerfum.

10 atvik

Tilraun til yfirtöku

Árangurslausar tilraunir til að taka yfir tölvukerfi fórnarlamba.

6 atvik

Upplýsingasöfnun

Söfnun upplýsinga um veikleika og netumferð án heimildar.

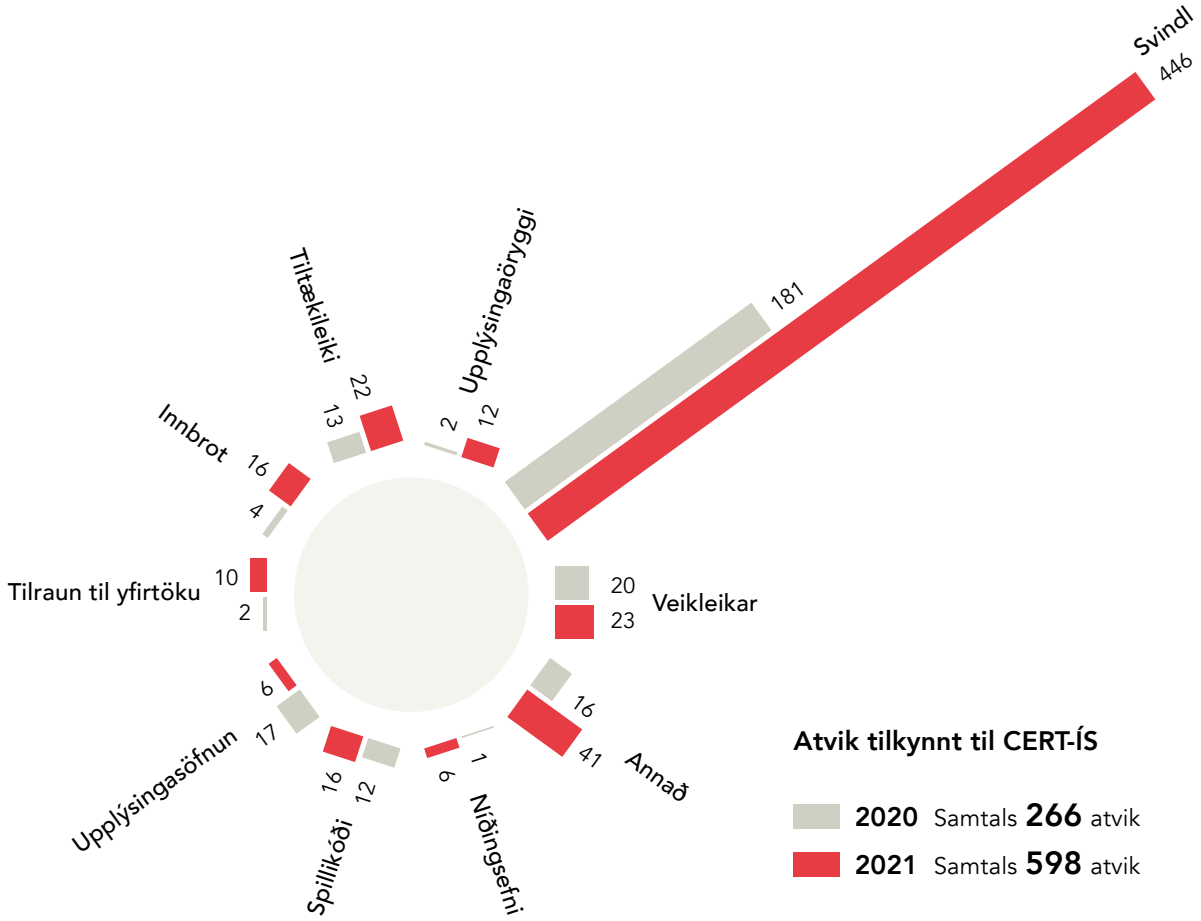
41 atvik

Annað

Aðgangur að upplýsingum eftir ólöglegum leiðum, gagnatap og gagnalekar.

Samtals: 598 atvik

Tölfræðin gefur okkur góðar vísbendingar um þá þróun sem er að verða á netárásum á Íslandi. Vert er þó að taka fram að aðeins er um tilkynnt atvik að ræða – atvikin geta verið fleiri en hér segir. Því er mikilvægt að öll atvik séu tilkynnt inn til okkar.



Engar opinberar tölur eru til um hve margar tölvur eru í notkun á Íslandi. Eitt er þó víst að langflest störf í dag eru háð öruggu tölvukerfi og aðgengi að internetinu. Nánast öll viðskipti fara fram í gegnum tölvukerfi. Aðgangs- og lyklakerfi byggja á tölvum, fjölmiðlar reiða sig á tölvukerfi til að geta sent út fréttir og umferðastýringar í sjó- og flugsamgöngum eru háðar upplýsingatækni með einum eða öðrum hætti.

Árið 2021 voru skráðar 598 tilkynningar um atvik inn til CERT-ÍS. Það er rúmlega tvöföldun í fjölda atvika frá 2020. Líklegt er að rekja megi þessa gríðarlegu fjölgun á tilkynningum til tveggja þátta, annars vegar almennrar aukningar á atvikum tengdum netöryggi í heiminum og hins vegar að meiri vilji er hjá fyrirtækjum og stofnunum að tilkynna um atvik sem verða í þeirra kerfum.

Áberandi er að mesta aukning tilkynninga er í flokki svindls á netinu. Þar falla undir t.d. vefveiðar þar sem reynt er að safna viðkvæmum upplýsingum með því að villa á sér heimildir til dæmis í gegnum tölvupóst eða með eftirmynd af þekktri síðu. Ein ástæða þessarar miklu aukningar eru staðgengilsþjónustur í lénaskráningum sem reknar eru á Íslandi og fela ekki eingöngu persónuupplýsingar venjulegs fólks heldur einnig þeirra sem stunda vafasamari iðju. Atvik sem snerta staðgengils-þjónustur sem staðsettar eru á Íslandi berast til CERT-ÍS þótt engin hýsing eða önnur þekkt tengsl séu við landið. CERT-ÍS hefur ekki lagaleg úrræði til að bregðast við slíkum tilkynningum.

Staðgengilsþjónustur (e. privacy and proxy services) er hægt að nýta til að dylja persónu-upplýsingar sem krafist er við skráningu léna. Í staðinn fyrir þann sem skráir lénið koma tengiliðaupplýsingar staðgengilsþjónustunnar í staðinn. Engar reglur eða lagalegar kröfur eru um slíka starfsemi á Íslandi og getur reynst erfitt að koma skilaboðum til þeirra sem raunverulega standa á bak við mörg lén.

Samkvæmt lögum ber fjarskiptafyrirtækjum og rekstraraðilum nauðsynlegrar þjónustu að tilkynna atvik til CERT-ÍS. Þessu til viðbótar hvetur CERT-ÍS aðrar stofnanir og fyrirtæki að tilkynna um atvik tengd netöryggismálum til að geta haldið úti sem réttastri mynd af stöðu netöryggismála á Íslandi hverju sinni.

Það er erfitt að reikna út fjárhagslegt tap sem verður vegna netglæpa. Sérstaklega þar sem beint fjárhagslegt tap gefur ekki rétta mynd af raunverulegu tapi sem verður vegna netárásar. Tap á gögnum, stöðvun á vinnu og úrvinnsla sem getur orðið til vegna netárásar getur leitt af sér gífurlegan kostnað fyrir fórnarlambið sem erfitt getur verið að fá bætt. Alþjóðlegar rannsóknir sýna að allt að 60% smærri fyrirtækja sem verða fyrir netárás hætta starfsemi innan sex mánaða frá því að árásin var gerð. Því fylgir einnig áfall, andlegt álag og streita að verða fyrir netárás sem þarf að vinna úr.

Evrópsku netöryggisstofnunin, (European Union Agency for Cybersecurity (ENISA)), mat tap ríkja í Evrópu vegna netglæpa um 1,6% af vergri landsframleiðslu (GDP) á ári. Tveimur árum síðar, 2018, var mat áströlsku ríkisstjórnarinnar að tap samfélagsins væri 1,9% af GDP á ári vegna netglæpa.

Ef við heimfærum þessar tölur á Ísland sést að um töluverða fjármuni er að ræða. Með því að gera ráð fyrir að um 1,5% af GDP á Íslandi tapist vegna netglæpa eru það um 40 milljarðar sem tapast á ári. Vegna eðli netglæpa er það samstarfsverkefni samfélagsins í heild að huga að vörnum gegn netógnum.

Tvö stór mál komu upp á síðasta ári sem fjallað verður sérstaklega um síðar í skýrslunni. Það eru DDoS árásir á fjármálageirann og Log4j veikleikinn. Það er staðreynd að alvarlegir veikleikar eða áhætta geti komið í ljós hvenær sem er og einnig að innviðir okkar verði bein skotmörk netglæpamanna. Því er mikilvægt að vera ávallt tilbúin að bregðast við.

Log4j-veikleikinn

Árið 2021 var í fyrsta skiptið virkjað óvissustig almannavarna vegna netógnar á Íslandi, þegar í ljós kom mjög alvarlegur veikleiki í kóðasafninu Log4j. Veikleikinn hafði áhrif um allan heim og í langflestum kerfum mátti finna einhvern búnað eða forrit sem þurfti að uppfæra eða fjarlægja.

Þann 10. desember var opinberað að veikleiki með alvarleikann 10 af 10 mögulegum hefði fundist í kóðasafninu og uppfærsla gefin út. Í kjölfarið hófst vinna kerfisstjóra í flestöllum fyrirtækjum í heiminum við finna öll forrit sem nýttu safnið, uppfæra þau, fjarlægja eða koma í veg fyrir áhrif með öðrum hætti. Eins og oft er með veikleika fundust í kjölfarið tveir minni veikleikar í sama kóðasafni og þurfti að endurtaka uppfærslur á mörgum kerfum. Birgjar upplýsingatæknigeirans voru enn að gefa út uppfærslur í byrjun 2022.

Dæmi um hvernig veikleikinn í Log4j var misnotaður var að koma fyrir gagnagíslatökubúnaði (e. ransomware) og senda fjárkúgunarkröfu í kjölfarið, stela kerfis skilríkum, taka yfir stjórn á veikum kerfum og stela gögnum þeirra. Tvö stór erlend atvik eru rakin beint til þessa veikleika.

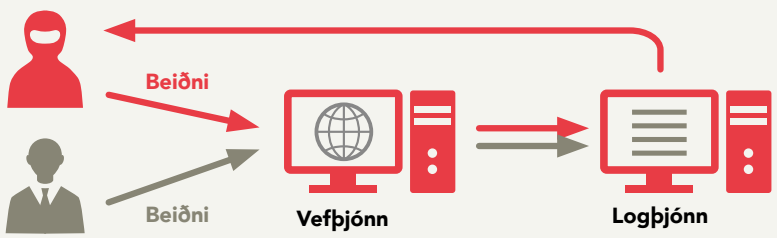
Þar sem útbreiðsla algengra forrita og kóðasafna er mjög mikil er aðeins tímaspursmál hvenær næst komi álíka stór veikleiki upp. Ísland þarf að vera undir það búið að grípa til markvissra aðgerða eins og rekstraraðilar gerðu síðastliðinn desember, þar sem tugir ef ekki hundruðir íslenskra tæknimanna lögðu nótt við dag í aðdraganda jóla til að bregðast við og tryggja kerfi sín. Enn fremur má færa fyrir því rök að leita ætti allra leiða til að minnka vinnu sem þessa næst þegar jafn alvarlegur veikleiki skýtur upp kollinum.

Eitt að þeim verkfærum sem við höfum til að takast á við útbreidd atvik sem þetta er að virkja viðbragðsstig Almannavarna í samræmi við lög nr. 82/2008. Í viðbragðsáætlun eru skilgreind þrjú stig, óvissustig, hættustig og neyðarstig. Á óvissustigi hefst samráð milli Almannavarna og CERT-ÍS. CERT-ÍS fer með samhæfingarhlutverkið og reglulega er framkvæmt stöðumat. Á hættu- og neyðarstigi er samhæfingar- og stjórnstöð Almannavarna virkjuð, en hún sér um samræmingu og stjórnun allra aðgerða með ráðgjöf og stöðumati frá CERT-ÍS.

Af hverju nota svo mörg kerfi log4j?

Kóðasafnið einfaldar mjög skráningu í atburðaskrá, og í stað þess að hver forritari skrifi sína eigin útgáfu af slíkri virkni er mun fljótlegra og yfirleitt öruggara að nýta það sem þegar er til.
Ekki finna upp hjólið aftur.

Dæmi um árás sem nýtti veikleikann í Log4j



Álagsárásir á íslenska fjármálainnviði

Álagsárásir (e. DDoS – Distributed Denial of Service attacks) eru árásir sem trufla aðgang að þjónustu yfir internetið.

Síðustu ár hefur verið gífurleg aukning á að glæpahópar noti álagsárásir í þeim tilgangi að krefjast lausnargjalds af fórnarlambinu (e. ransom DDoS/RDDoS). Algengast er að glæpahópurinn framkvæmi stutta árás til að sýna getu sína til að framkvæma DDoS. Í kjölfarið er send hótun um frekari árásir nema fórnarlambið greiði fjárkúgunarkröfuna. Þekkt er að aðilar kaupi RDDoS árásir af sérhæfðum glæpahópum til að ráðast á ákveðið fyrirtæki.

Yrkjanet

Það getur verið gífurlega erfitt að greina hver stendur á bak við álagsárás nema í þeim tilvikum þar sem hótunarbréf eru send. Ástæða þess að erfitt getur verið að greina hver gerir álagsárás er að þær eru oft framkvæmdar með hjálp yrkjaneta (e. Botnet) eða nýta netþjóna með veikleika til að endurvarpa umferð á fórnarlamb álagsárásanna (e. reflection/amplification attacks). Árásin virðist koma frá fjölda mismunandi upphafsstaða sem lítið eða ekkert eiga sameiginlegt, raunverulegir gerendur eru svo faldir á bak við keðju af netþjónum í mismunandi lögsögum, sem gerir rakningu erfiða. Í þeim tilvikum getur reynst óljóst hver þróun árásarinnar verður.

Álagsárásir á íslenska fjármálainnviði

Í september 2021 urðu íslensk greiðslumiðlunarkerfi fyrir endurteknum álagsárásum sem hafði meðal annars í för með sér að öll greiðslukort voru ónothæf yfir stutt tímabil á laugardagskvöldi 11. september.

Greiðslumiðlanir, bankar og fjarskiptafyrirtæki brugðust hratt við þessum árásum og unnu sérfræðingar þeirra að því að hrinda árásunum yfir nokkurra vikna tímabil. Það má því segja að þótt að áhrifin hafi verið mikil hafi tekist að halda þeim í lágmarki vegna þessara viðbragða.

Þegar slík árás dynur yfir eitt eða fleiri þjónustufyrirtæki má ekki gleyma því hversu víðtækur skaðinn er. Laugardagskvöld eru sá tími þar sem mest er að gera á veitingahúsum, og ef tafir eru við greiðslu leiðir það t.d. til þess að borð losna ekki á réttum tíma. Erfitt er að meta heildarkostnað og tap vegna slíkra atburða.

Ekki hefur verið hægt að greina hver framkvæmdi árásirnar gegn fjármálakerfunum né tilgang þeirra.

Árásir sem byggja á magni
(e. volume based)
Markmið: að fullnýta bandvídd
- UDP flóð
- ICMP flóð
- Flóð af eftirlíkingum *(e. spoofed packets)*

Árásir byggðar á samskiptareglum
(e. protocol attacks)
Markmið: að fullnýta auðlindir
- SYN flóð
- Árás með tvístruðum pökkum *(e. fragmented packets)*
- Banabank *(e. Ping of Death)*
- Strumpaárás *(e. Smurf DdoS)*

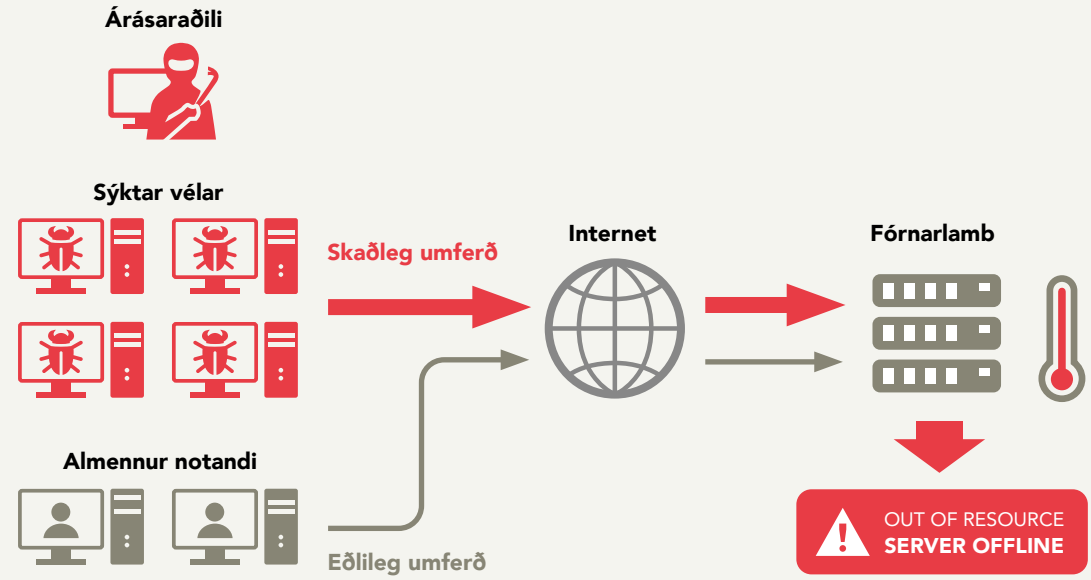
Árásir á notkunarlagi
(e. application layer)
Markmið: að valda kerfishruni
- Lítil og hæg árás *(e. low-and-slow)*
- GET/POST flóð
- Árás á veikleika

Þróun árása

Álagsárásir hafa þróast síðustu ár í að verða sérsniðnar að fórnarlambinu og oft notaðar fleiri aðferðir (e. multivector) við framkvæmd árásanna en áður þekktist. Með öðrum orðum þá framkvæmir árásaraðilinn árás sem hann telur duga til að trufla þjónustugetu fórnarlambsins. Ef sú árás dugar ekki er breytt um tegund og styrk þar til árásin hefur náð markmiðum sínum. CERT-ÍS hefur séð sérsniðnar álagsárásir framkvæmdar á Íslandi.

Samkvæmt greiningu Netscout voru 5,4 milljón álagsárásir gerðar á fyrri hluta ársins 2021. Flestar árásirnar voru framkvæmdar með aðstoð yrkjaneta. Einnig var áberandi að árásum sem nota mismunandi aðferðir (e. multivector) fjölgaði meira en tvöfalt. CERT-ÍS framkvæmdi ástandskönnun á hvernig vörnum gegn álags-árásum er háttað hér á landi og viðhorfum til ógna á seinni hluta árs 2021. Voru allir þátttakendur sammála að líklegt er að fjöldi álagsárása muni fara vaxandi á komandi árum og að álagsárásir muni halda áfram að þróast tæknilega.

Ferli DDoS árásar



Öryggi í fjarvinnu

Síðustu ár hefur það færst í aukana að fyrirtæki og stofnanir bjóði starfsfólki sínu að vinna heiman frá sér. Óhætt er að segja að COVID-19 heimsfaraldurinn hafi hraðað þessari þróun.

Þessari þróun fylgja nýjar áskoranir á ýmsum sviðum meðal annars á sviði tölvuöryggis. Starfsfólk þarf að vinna með gögn á tölvunni sinni sem leynd hvílir yfir, t.d. persónugreinanleg gögn, viðskiptaskjöl og allskonar skjöl um hugverk sem eru í stöðugri þróun.

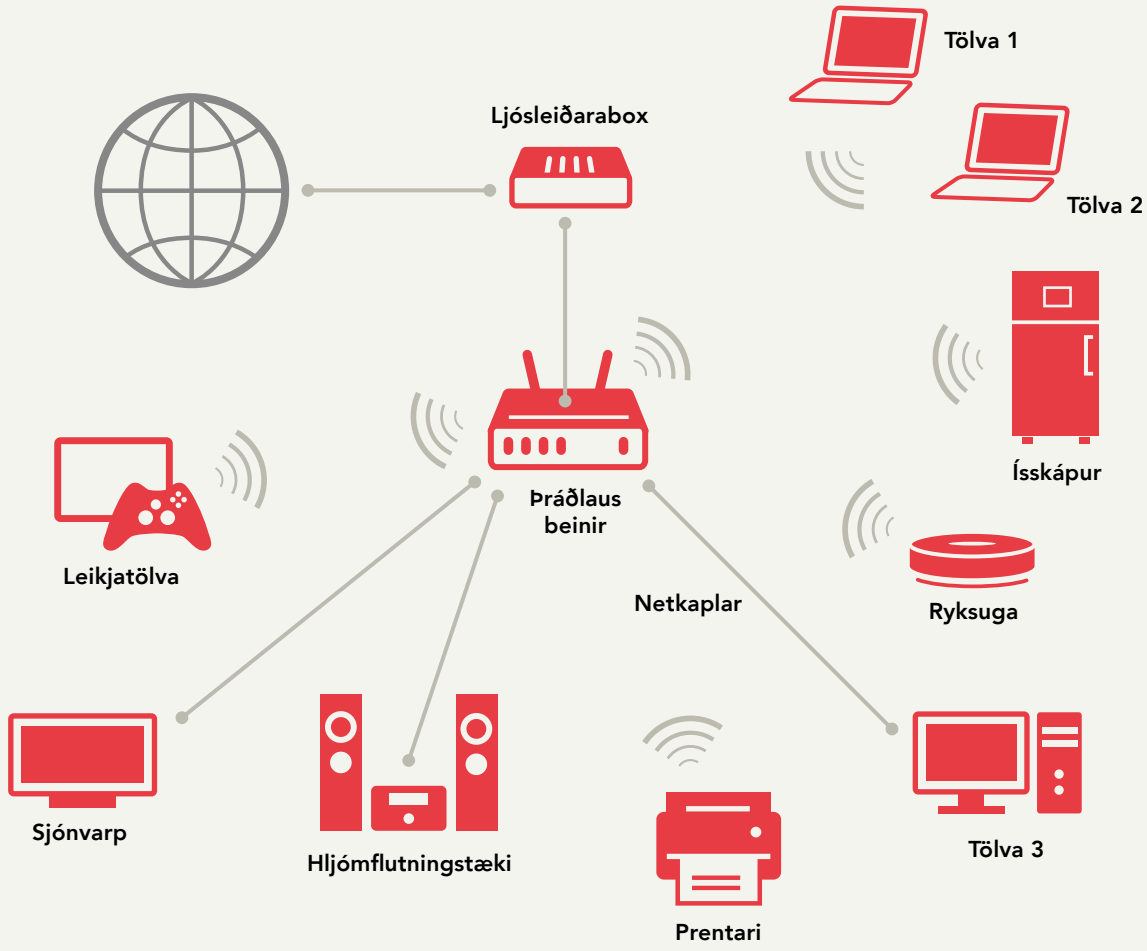
Þegar vinnudagurinn fer fram á skrifstofum fyrirtækja eða stofnana er séð til þess að tölvu- og netkerfið sé öruggt fyrir starfsfólk sem er að meðhöndla viðkvæm gögn. Það á ekki við þegar unnið er að heiman, þar sem starfsmenn tengjast sínu eigin heimaneti til að vinna vinnuna sína. Mikilvægt er að atvinnurekendur hugsi út í net- og tölvuöryggi þegar fólk vinnur heiman frá sér.

Mikilvægt er að aðgengi að tölvunni sé takmarkað, hún á ekki að vera til notkunar fyrir neinn nema starfsmanninn sjálfan. Gagnageymsla tölvunnar ætti einnig að vera dulrituð ef hún kynni að glatast en öll helstu stýrikerfi bjóða upp á það í dag. Einnig er mikilvægt að muna að aðgengi að viðkvæmustu gögnum og forritum gæti þurft að takmarka. Þar sem hægt er ætti að nota fjölþátta auðkenningu eða skilríki sem gera stuld á auðkennum erfiðari.

Internettengingar heima hjá fólki og snjalltæki sem tengjast sama þráðlausa heimaneti geta verið leið inn á allar tölvur fyrirtækisins eða stofnunarinnar. Þegar margir aðilar nota sama net skiptir máli hvað hver og einn er að gera. Er t.d. einhver heimilismaður að hala niður óþekktum hugbúnaði eða heimsækja óöruggar síður? Ef óværa nær fótfestu á einni tölvu getur hún dreift sér á aðrar tölvur og búnað sem tengd eru sama neti. Mikilvægt er að vélar séu með virka eldveggi og varnir gegn óværum en bestu lausnirnar í dag kallast endapunktsvarnir (e. end point protection) og veita mikið öryggi séu þær rétt settar upp og vaktaðar.

Til að auka öryggi sitt nýta margir vinnustaðir sýndareinkanet (e. Virtual Private Network), þá er hluti eða öll umferð frá tölvunni dulrituð og send í gegnum net atvinnurekandans. Með notkun VPN er hægt að nota kerfi sem eru sérstaklega varin. Ef öll umferð er flutt um VPN veitir það ákveðna vörn gegn hlerunum og breytingum sem og öryggisvöktun verður markvissari.

Fjölþættar tengingar heimanets



Sviðshópar og upplýsingaskipti

CERT-ÍS heldur utan um sviðshópa mikilvægra innviða þar sem áhersla er lögð á að efla netöryggisvarnir og viðbragðsgetu Íslands í netöryggisatvikum. Þeim markmiðum er meðal annars náð með því að hvetja til tæknilegs samráðs og að skiptast á upplýsingum sem varða net- og upplýsingaöryggi. Hóparnir munu móta sameiginlega sýn á þróun netöryggismála innan síns sviðs á Íslandi, til dæmis um hvaða upplýsingum ætti að deila sín á milli til að vera til gagns, undirbúa samhæft viðbragð vegna alvarlegra atvika og taka þátt í æfingum tengdum því.

Samvinna og upplýsingaskipti skipta miklu mál þegar kemur að net- og upplýsingaöryggi. Það sem ógnar einum getur einnig ógnað öðrum. Að skiptast á upplýsingum stuðlar að bættu öryggi allra sem taka þátt samstarfinu. Upplýsingaskipti koma einnig í veg fyrir að margir aðilar endurtaki sömu greiningarvinnu sem getur reynst tímafrek. Þess í stað samnýta aðilar upplýsingar til að efla skilning og varnir innan hópsins sem heildar.

Ein forsenda upplýsingaskipta er að traust ríki á milli allra þátttakenda. Aðilar þurfa að sjá hag sinn í að taka þátt í upplýsingaskiptunum. Það þýðir að allir aðilar leggja sitt af mörkum svo samstarfið nái tilætluðum árangri og virða traust og trúnað annarra.

Þó að tölvupóstur og netspjall séu til margs nytsamleg hafa slík frjáls samskiptaform ákveðna veikleika þegar kemur að viðbrögðum. Með því að nota formleg upplýsingasnið og sérhæfðari tól til miðlunar er hægt að auðvelda ýmsa vinnu, svo sem stýrðari dreifingu, sjálfvirka vinnslu svo sem viðvaranir og tengingu við önnur atvik og eldri mál.

Með því að taka þátt í formlegu upplýsingaskiptaneti með CERT-ÍS eykst geta okkar til að miðla sem réttastri mynd af stöðu Íslands í netöryggismálum.

Lykilorðabankar

Í daglegu lífi treystum við á notendanöfn og lykilorð til að tengjast flestum okkar aðgöngum á internetinu, hvort sem það séu samfélagsmiðlar, tölvupóstþjónusta, mynda- og gagnageymslur eða önnur þjónusta eða smáforrit. Á hverju ári verða margir gagnalekar þar sem lykilorðum notenda er lekið. Geta þá glæpahópar nýtt sér lykilorðin til þess að komast inn á aðganga fórnarlamba sinna. Þar sem fólk á það til að endurnýta lykilorðin sín eða nota mjög svipuð lykilorð auðveldar það glæpahópum að ná tökum á öðrum aðgöngum fórnarlambsins en þeim sem gagnalekinn nær til.

Til eru margar aðferðir við að verja sína aðganga eins og að hafa flókin lykilorð, fjölþátta auðkenningu og að eiga lykilorðabanka.

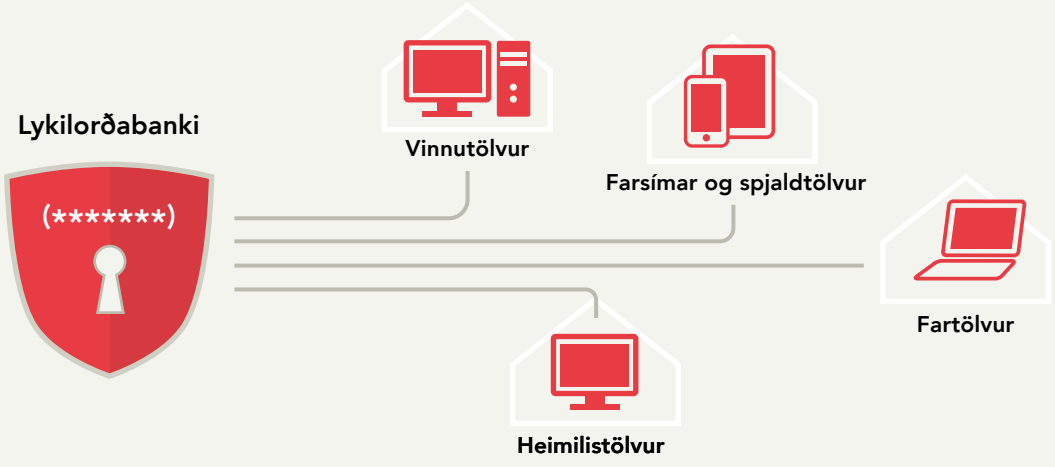
Lykilorðabankar gera fólki kleift að geyma innskráningarupplýsingar fyrir allar síður og þjónustur á einum öruggum stað. Ef einstaklingur notar lykilorðabanka getur hann látið bankann fylla út notendanöfn og lykilorð fyrir aðganga. Það þýðir að hvert og eitt lykilorð getur verið mun lengra og flóknara, þar sem lykilorðabankinn man það fyrir fólk. Einnig bjóða sumir lykilorðabankar upp á að búa til ný lykilorð og þá þarf ekki að byggja á ímyndunaraflinu heldur er hægt að fá flókið lykilorð af hæfilegri lengd sjálfkrafa. Aðeins þarf að muna eitt lykilorð, lykilorðið fyrir lykilorðabankann sjálfan. Mikilvægt er síðan að verja lykilorðabankann með fjölþátta auðkenningu.

Þegar búið er til lykilorð fyrir lykilorðabankann er mikilvægt að velja sterkt lykilorð sem hægt er að muna. Það er algeng mýta að lykilorð eigi að vera flókin, samhengislausir stafir og tákn sem er varla hægt að muna röðina á. Í dag eru löng einföld lykilorð talin sterkari en stutt og flókin. Þannig er betra að mynda samhengislausa setningu úr nokkrum orðum með mislöngum tölum blönduðum inn frekar en að velja fáa stafi og tákn sem erfitt er að muna.

✗ GK"$/45gS
✓ Jolasveinninn323elskarpaskamat84i109oktober

Algeng og slæm lykilorð

1. 123456
2. Qwerty
3. Password
4. Nafn á börnum/mökum/gæludýrum
5. Uppáhalds íþróttalið/hljómsveit
6. <orð><tala>



Gagnagíslataka

Það er sífellt algengara að glæpamenn noti hótanir og fjárkúgun við að hafa fé af fyrirtækjum, t.d. með gagnagíslatöku (e. ransomware attack). Hafa glæpamennirnir þá náð að komast yfir gögn fyrirtækisins, dulkóðað þau eða eytt af netþjóni. Senda þeir síðan greiðsluleiðbeiningar á fyrirtækið og lofa að gegn greiðslu muni fórnarlambið aftur fá aðgang að gögnunum sínum. Einnig er orðið algengt að hótað sé að birta gögnin opinberlega ef fyrirtæki greiði ekki kröfuna sem getur haft alvarlegar afleiðingar séu gögnin viðkvæm, t.d. persónugreinanlegar upplýsingar. Stjórnir og eigendur fyrirtækja þurfa því að líta inn á við og skoða hversu vel í stakk búið fyrirtækið þeirra er til að bregðast við þess háttar árás.

Það er ekki hægt að gera þá kröfu á stjórnendur og yfirmenn fyrirtækja að fara í mjög tæknilegt samtal þegar kemur að tölvuöryggi síns fyrirtækis. Aftur á móti eru nokkrar spurningar sem þarf að hafa í huga, sérstaklega þegar fyrirtæki lenda í fjárkúgunartilburðum:

1. **Er fyrirtækið með afrit af þeim gögnum sem nauðsynlegt er að hafa til að tryggja rekstur fyrirtækisins og eru þau hýst á öruggum stað?**
   - Er búið að skilgreina hvaða gögn eru ómissandi fyrir reksturinn? Hve oft eru afrit tekin af þeim gögnum?
   - Hvar eru afritin geymd, eru þau óaðgengileg glæpamönnum, á ótengdum tækjum eða í skýjalausnum? Hvað mun taka langan tíma að fá aðgang að afritunum?
2. **Eru til ítarlegir ferlar sem fara í gang þegar gerð er tilraun til fjárkúgunarárásar á fyrirtækið?**
   - Skilgreina ferlarnir hvenær á að hafa samband við allar þær deildir sem áætlunin nær yfir? T.d. stjórnendur, lögfræðinga og markaðsdeildina?
   - Er verkefni allra skilgreint? Hvenær á markaðsdeildin að útbúa fréttatilkynningu, hvaða eftirlitsstjórnvald þarf að hafa samband við?
3. **Hver tekur lokaákvörðun um hvort fyrirtækið greiði fjárkúgunarkröfuna eða ekki?**
   - Hversu lengi getur fyrirtækið starfað án þeirra gagna sem voru tekin?
   - Ef gögn myndu leka út gæti orðspor fyrirtækisins staðið það af sér?

Rétt er að taka fram að CERT-ÍS ráðleggur aldrei að greiða glæpamönnum sem reyna að kúga fé út úr fyrirtækjum lausnarfé. Ekki er tryggt, þó fjárkúgunarkrafan sé greidd, að fyrirtæki fái gögnin sín til baka eða gögnunum verði ekki lekið út. Einnig gæti það aukið líkurnar á að fyrirtækið verði að skotmarki aftur seinna meir.

Netglæpamenn hafa í mörg ár verið að þróa bestu leiðina til að þvinga fyrirtæki til að verða við kröfum sínum. Það þýðir að glæpamennirnir hafa oft vitneskju um hve hátt lausnargjald fórnarlambið getur greitt. Það getur þýtt að það sé freistandi fyrir fyrirtæki að greiða kröfuna í þeirri von að halda rekstrinum áfram óhindrað. Aftur á móti er ekki óalgengt að gögnin séu nokkrar vikur á leiðinni frá glæpamönnunum eða komi sködduð til baka eftir að greiðsla er innt af hendi. Engin trygging er fyrir því að geta hafið störf strax þó látið sé undan fjárkúgun glæpamannanna.

Öll fyrirtæki geta orðið fyrir gagnagíslatöku. Skiptir þar ekki máli stærð eða starfsumhverfi fyrirtækisins. Því verða allir stjórnendur og eigendur fyrirtækja að móta stefnu, viðbragðsáætlun og verkferla sem eru virkjaðir við netárásir.

Gagnagíslataka

2021

JANÚAR 5 stöðugildi

- Rekstraraðilar nauðsynlegrar þjónustu útnefndir
- Ný reglugerð um CERT-ÍS (480/2021)
- Lög um íslensk landshöfuðlén (54/2021)
- Ný lög um Fjarskiptastofu (75-2021)
- CERT-ÍS flytur í nýtt húsnæði
- Álagsárásir á Fjármálainnviði á Íslandi
- Sviðshópur fjármálainnviða tekur til starfa
- Innbrot í tölvupóstþjóna HR
- Netöryggisstefna Íslands 2021–2036
- Veikleiki í Log4j
- Innbrot í kerfi Strætó bs.

DESEMBER 8 stöðugildi