CERT·IS

Ársskýrsla 2023

CERT-IS er svið undir Fjarskiptastofu. Málefni netöryggis heyra undir háskóla-, iðnaðar- og nýsköpunarráðuneytið (HVIN).

Ávarp sviðsstjóra

CERT·IS

ÁRSSKÝRSLA 2023

Árið 2023 reyndist viðburðarríkt fyrir netöryggissveitina CERT-IS. Upprunalegum áætlunum um uppbyggingu sveitarinnar var flýtt í kjölfar innrásar Rússa í Úkraínu árið áður. Lögð var lykiláhersla á að tryggja getu sveitarinnar til að þjónusta sviðshópa mikilvægra innviða við atvikameðhöndlun auk þess að efla getu hennar til að greina ástand netöryggismála fyrir íslenska netumdæmið í heild sinni. Reyndust þessar aðgerðir mikilvægar til að mæta auknum kröfum og verkefnum í erlendu og innlendu samstarfi sem CERT-IS er þátttakandi í.

Megináhersla hefur verið lögð á að koma á fót öflugu teymi sem hefur getu til að sinna atvikameðhöndlun með réttum ferlum og tólum. Búið er að innleiða nýtt atvikaskráningarkerfi sem auðveldar utanumhald mála sem tengjast hverju atviki fyrir sig og einfaldar alla tölfræðivinnslu í kjölfarið. Þjónusta CERT-IS var bætt á árinu með fjölgun starfsfólks á vakt og nú sinna tveir dagvakt hverju sinni. CERT-IS er stolt af því að hafa unnið til UT-Messu verðlauna fyrir bestu stafrænu þjónustuna snemma árs 2023. Var það mikil viðurkenning á stefnu sveitarinnar og á sama tíma mikil hvatning til teymisins um að gera enn betur.

Þessi meðbyr nær til fleiri anga netöryggissamfélagsins þar sem greina má mikla vitundarvakningu um málaflokkinn innan alls netumdæmisins. Skiptir þá litlu hvort horft sé til fyrirtækja, stofnana eða inn í stjórnsýsluna sjálfa. Greina má meiri vilja innan netumdæmisins til að skiptast á mikilvægum upplýsingum varðandi netöryggisatvik og veikleika og sú þróun styrkir tvímælalaust viðnámsþrótt netumdæmisins í heild sinni.

Mikil áhersla var lögð á alþjóðlegt samstarf á árinu. Hefðbundin landamæri eiga ekki við í netheimum og því mjög mikilvægt að eiga í nánu og traustu samstarfi við okkar helstu bandalagsþjóðir

er kemur að netöryggis- og varnarmálum. CERT-IS tók þátt í vaxandi samstarfi Norðurlandanna á sameiginlegum vettvangi þeirra og tók fullan þátt í stefnumótun og vinnustofum um ógnargreiningar ásamt stórri netöryggisæfingu Norðurlandanna og Netöryggisstofnunar Bandaríkjanna (CISA).

CERT-IS tók einnig virkan þátt í samstarfi Íslands um netöryggismál á sviðum NATO samstarfsins. Ber þar helst að nefna þátttöku Íslands í Skjaldborginni (e. Locked Shields). Er þar um að ræða stærstu netöryggisæfingu sem haldin er ár hvert og fékk starfsfólk CERT-IS og annað úrvalslið íslenskra fyrirtækja og stofnana að taka þátt með liði Svíþjóðar. Fór það svo að þetta sameiginlega lið Íslands og Svíþjóðar stóð uppi sem sigurvegari Locked Shields 2023 og er það frábær árangur sem við megum vera stolt af.

Leiðtogafundur Evrópuráðsins var haldinn í Hörpu í Reykjavík í maí 2023. Fundurinn krafðist gífurlegs undirbúnings sem starfsfólk Ríkislögreglustjóra leiddi með miklum sóma. CERT-IS var fengið að borðinu til að undirbúa og greina helstu netógnir í kringum fundinn. Sviðshópar mikilvægra innviða sönnuðu gildi sitt í þessu verkefni þar sem beinar boðleiðir milli rekstraraðila nauðsynlegra upplýsingatæknikerfa gátu stillt saman strengi og staðið vaktina á meðan leiðtogafundurinn var haldinn. Helstu spár um eðli netárása samhliða fundinum gengu að megninu til eftir þar sem ógnarhópar hliðhollir rússneskum málstað héldu úti dreifðum álagsárásum á íslensk fyrirtæki og íslenskar stofnanir. Árangur þeirra verður að teljast minni háttar í samhengi við tilefnið og eiga íslenskir rekstraraðilar hrós skilið fyrir undirbúning, viðbragð og almenna aðkomu sína að þessum fundi.

Ávallt má þó gera betur. CERT-IS mun halda áfram að leggja áherslu á að bæta þjónustu til sviðshópa og auka burði sveitarinnar til að bæta ástandsvitund netöryggismála öllum til hagsbóta. Bæta þarf getu sveitarinnar og íslenska netöryggissamfélagsins til að geta greint

ógnarvísa sem leynast innan íslenska netumdæmisins. Hægt er að fylgja fordæmi nágrannaþjóða og innleiða snemmviðvörunarkerfi sem hefur það meginmarkmið að greina ógnir í netheimum og flagga þeim til réttra aðila. Þar hefur CERT-IS lykilhlutverki að gegna er varðar miðlæga samhæfingu og upplýsingaskipti.

Í hröðum vexti CERT-IS hefur komið í ljós hvar þarf að slípa ferla og skilgreina betur hvaða upplýsingar um atvik er æskilegt að tilkynna til CERT-IS og hvenær. Það er hagur allra að viðeigandi upplýsingar berist hratt og vel til réttra aðila. Er það því forgangsmál í samvinnu við hluthafandi aðila að skýra betur þau viðmið sem notast á við þegar tilkynnt er um atvik. Verða niðurstöður þeirrar vinnu kynntar öllum sviðshópum sérstaklega.

Fyrir liggur uppfærsla á netöryggislöggjöfinni með innleiðingu á NIS2 Evrópuregluverkinu í íslensk landslög. Er einsýnt að með innleiðingu þeirra mun mengi aðila er falla undir regluverkið stóraukast frá því sem nú er og er mikilvægt að stjórnvöld og stofnanir eigi náið samtal við aðila netumdæmisins samhliða innleiðingunni. NIS2 regluverkið kemur til með að stýra starfsemi CERT-IS að miklu leyti inn í framtíðina og má reikna með verulega auknum kröfum til CERT-IS.

Starfsfólk CERT-IS er spennt fyrir framhaldinu. Fram undan er afrakstur þess uppbyggingarstarfs sem hefur átt sér stað undanfarin ár: Betri sýn á ástand netöryggismála, aukið virði upplýsinga úr tólum sveitarinnar auk enn betra samstarfs við íslenska netöryggissamfélagið. CERT-IS þakkar samstarfið árið 2023.

Virðingarfyllst,
Guðmundur Arnar Sigmundsson
Sviðsstjóri CERT-IS

Árið í tölum

Líkt og undanfarin ár hefur fjöldi atvika aukist til muna milli ára sem er sama þróun og annars staðar í heiminum. Það er mikilvægt að halda vel utan um tölfræði netöryggisatvika á Íslandi svo hægt sé að bera þróunina hér saman við þá í öðrum löndum. Ef ákveðinn atvikaflokkur vex langt fram úr öðrum flokkum og úr takti við þróunina í löndunum í kringum okkur er brýnt að skoða það nánar og reyna að finna út hvað veldur aukningunni.

Sú tala sem sker sig mest úr er fjöldi svindla en árið 2023 var hann hærri en heildarfjöldi tilkynntra atvika árið 2022. Svindl eru í hraðri þróun og verða þau vandaðri með hverju árinu sem líður. Svindlin eru betur útfærð en áður og það er greinilegt að sum þeirra sem standa á bak við svindlherferðir gegn Íslendingum hafa kynnt sér aðstæður hér vel. Notkun rafrænna skilríkja var ný tegund svindla þar sem bragðvísi (e. social engineering) var beitt til að fá einstaklinga til að samþykkja trúanlega rafræna auðkenningu.

Fleiri flokkar tóku stökk og er þá vert að nefna innskráningartilraunir. Hluti þeirra átti sér stað í kringum Leiðtogafund Evrópuráðsins í maí sem beindi tvímælalaust kastljósi ógnarhópa að Íslandi. Það er áhyggjuefni hve mikil fjölgun var í tilkynntum innskráningartilraunum því ef aðeins ein slík heppnast getur mikið tjón hlotist af hjá þeim aðila sem herjað er á. Fjöldi innbrota jókst einnig milli ára en þó ekki hlutfallslega jafn mikið og fjöldi innbrotstilrauna, sem er jákvætt.

Mun fleiri spillikóðar fundust í kerfum hér á landi en árið á undan. Orsökin er líklega að hluta til aukin geta CERT-IS til að greina spillikóða í íslenskum kerfum. Fjölgun starfsmanna og betri kerfi hafa skilað sér í auknum afköstum á þessum vettvangi.

Bragðvísi er þegar sálfræðilegum aðferðum er beitt til að blekkja fólk svo það gefi frá sér viðkvæmar upplýsingar.

Síðasti flokkurinn sem vert er að nefna er nýuppgötvaðir veikleikar sem hægt er að nýta til árása eða innbrotstilrauna. Veigameiri erlendir aðgerðarhópar (e. APT groups) eru stöðugt að leita að veikleikum til að misnota. Til að verjast því hafa fyrirtæki og stofnanir verið duglegri í leit að veikleikum í sínum eigin kerfum og gert úrbætur til að koma í veg fyrir misnotkun. Þessar aðgerðir fyrirtækja gætu átt þátt í hástökkinu milli ára.

Líkt og annars staðar má sjá aukningu atvika á Íslandi; þó er gríðarlegur munur milli 2022 og 2023. Þróunina má að hluta til rekja til þess að CERT-IS er sífellt að bæta yfirsýn sína yfir íslenska netumdæmið auk fjölgunar í teyminu, betri kerfa og öflugrar greiningarfærni. Tilkynningum atvika frá fyrirtækjum, stofnunum og einstaklingum hefur einnig fjölgað til muna.

Atvik 2023 - *Atvik 2022*

24 atvik - *8 atvik*
Upplýsingaöryggi
Aðgangur að upplýsingum eftir ólöglegum leiðum, gagnatap og gagnalekar.

24 atvik - *26 atvik*
Tiltækileiki
Kerfi og þjónusta ekki aðgengileg af ytri ásetningi, t.d. álagsárásir þegar þjónusta tölvukerfa er vísvitandi skert með yfirálagi.

704 atvik - *422 atvik*
Svindl
Netveiðar þar sem reynt er að komast yfir viðkæmar upplýsingar, s.s. kortanúmer eða lykilorð.

17 atvik - *9 atvik*
Níðingsefni
Einelti, áreitni og eltihrellni. Auk þess barnaníðsefni og upphafning ofbeldis.

109 atvik - *28 atvik*
Veikleikar
Veikleikar sem hægt er að nýta til að brjótast inn í eða hafa áhrif á tölvukerfi annarra.

30 atvik - *18 atvik*
Innbrot
Innbrot í tölvukerfi hjá heimanotendum, fyrirtækjum eða rekstraraðilum.

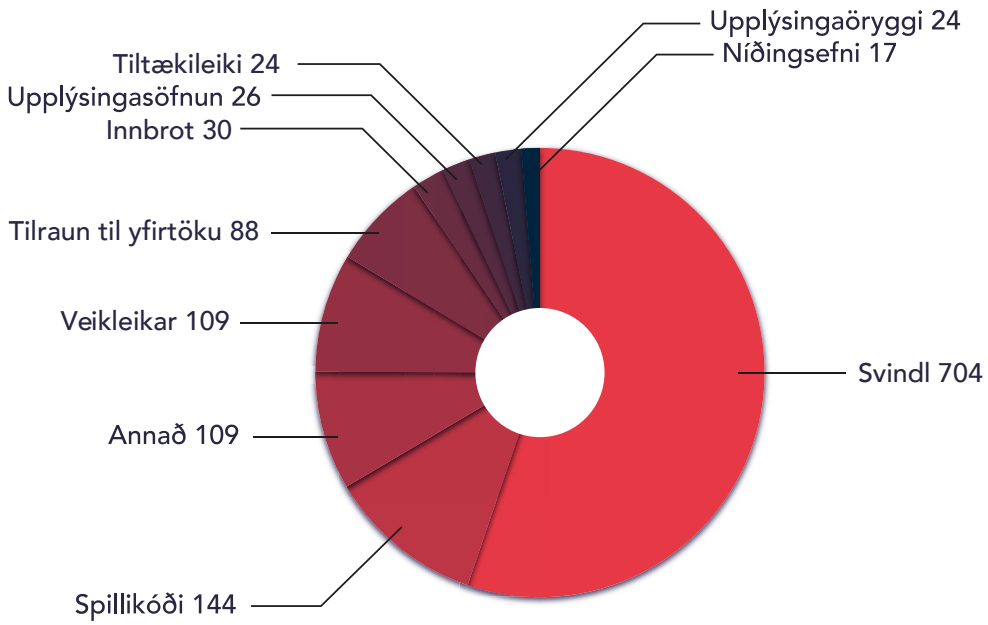
144 atvik - *26 atvik*
Spillikóði
Tölvuveirur og annar kóði sem notaður er til að eyðileggja eða ná stjórn á tölvukerfum.

88 atvik - *34 atvik*
Tilraun til yfirtöku
Árangurslausar tilraunir til að taka yfir tölvukerfi fórnarlamba.

26 atvik - *15 atvik*
Upplýsingasöfnun
Söfnun upplýsinga um veikleika og netumferð án heimildar.

109 atvik - *114 atvik*
Annað
Aðgangur að upplýsingum eftir ólöglegum leiðum, gagnatap og gagnalekar.

Samtals: **1.266 atvik 2023**



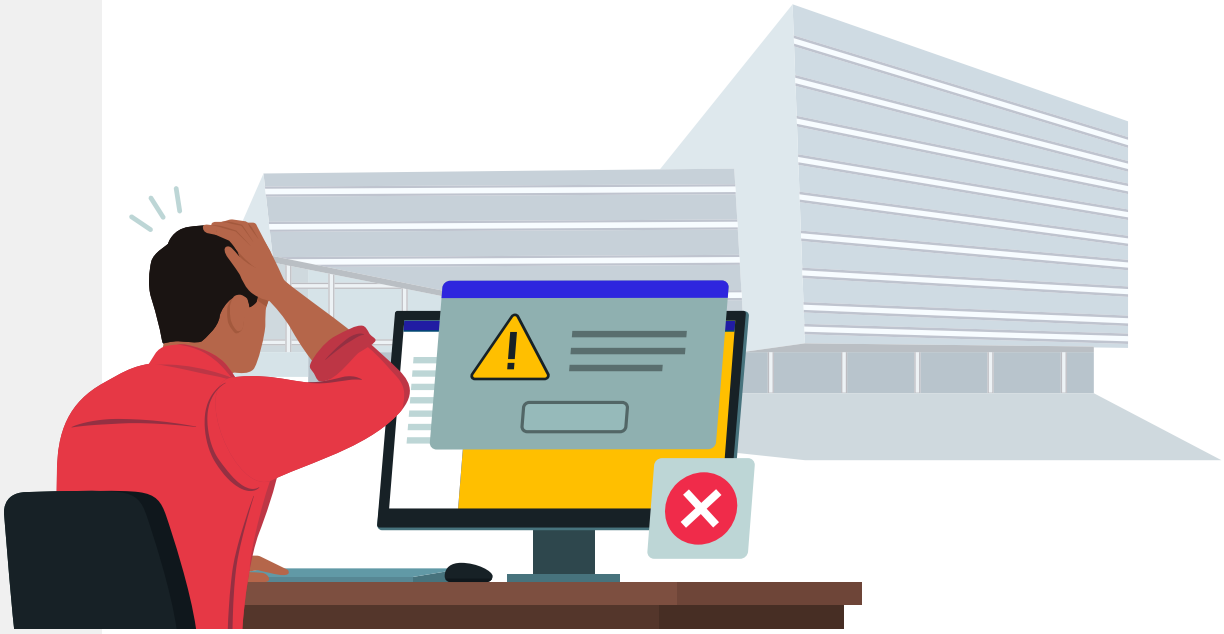
Leiðtogafundur

Árið 2023 var leiðtogafundur Evrópuráðsins haldinn í Reykjavík. Þetta var fjórði leiðtogafundurinn í sögu Evrópuráðsins og ein af stærstu samkomunum sem Ísland hefur haldið. Búist var við helstu leiðtogum allra Evrópulandanna. Umræðuefnið var annars vegar að skerpa á grunngildum ráðsins og hins vegar hvernig áframhaldandi stuðningi við Úkraínu yrði háttað. Því var talið líklegt að á meðan leiðtogafundurinn færi fram yrði Ísland skotmark ýmissa rússneskra ógnarhópa og sú varð raunin.

Í heildina var CERT-IS tilkynnt um 52 atvik í vikunni sem leiðtogafundurinn átti sér stað og er það 236% aukning frá hefðbundinni viku á svipuðum tíma. Stærstu atvikin voru dreifðar álagsárásir (e. DDoS attacks) og var þeim beint gegn vefsíðum ákveðinna stofnana með það að markmiði að trufla rekstur þeirra og starfsemi. Rússnesku ógnarhóparnir NoName057 og KillNet lýstu yfir ábyrgð á hluta árásanna.

Árásirnar beindust meðal annars gegn althingi.is, haestirettur.is, isavia.is, stjornarradid.is og cert.is. Þær gerðu vefsíður sem þær beindust gegn óstarfhæfar tímabundið og í sumum tilfellum höfðu árásirnar áhrif á net- og símasamband stofnana en ekki einungis vefsíðurnar. Auk álagsárásanna voru innskráningartilraunir framkvæmdar í vefgáttum sem nota rafræn skilríki, meðal annars island.is. Þessar tilraunir námu þúsundum og leiddu til tímabundinna truflana á þjónustu.

Þrátt fyrir ýmiss konar árásir og fjölbreytt skotmörk var skipulag og samvinna þeirra sem stóðu vaktina góð. CERT-IS var í stöðugum samskiptum við þjónustuhópa; öllum upplýsingum um árásir var miðlað um leið og þær bárust. Það tryggði yfirsýn yfir stöðuna og skilvirkar ráðleggingar, viðvaranir og hækkun áhættustigs. Í sumum tilfellum tókst að vara næsta skotmark álagsárásar við með nokkurra mínútna fyrirvara. Það lágmarkaði truflunina sem hlaust af árásinni því viðkomandi stofnun tókst að undirbúa viðbragðið.



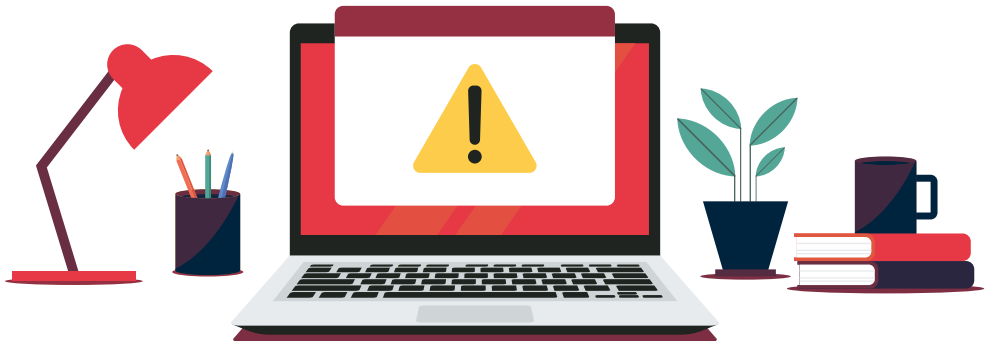
DDoS árásir

Heilt yfir gekk samhæfing og upplýsingamiðlun vel meðan á leiðtogafundinum stóð og eftir að honum lauk og mikill lærdómur var dreginn af viðburðinum.

Dreifðar álagsárásir (DDoS) eru algeng árásarleið þar sem vefsíður eða þjónustur sem styðjast við internetið verða tímabundið óvirkar. Færri tilkynningar bárust um DDoS árásir á Íslandi 2023 heldur en árið á undan. Flestar árásirnar sem gerðar voru árið 2023 beindust gegn ríkisstofnunum og voru áberandi í kringum leiðtogafundinn.

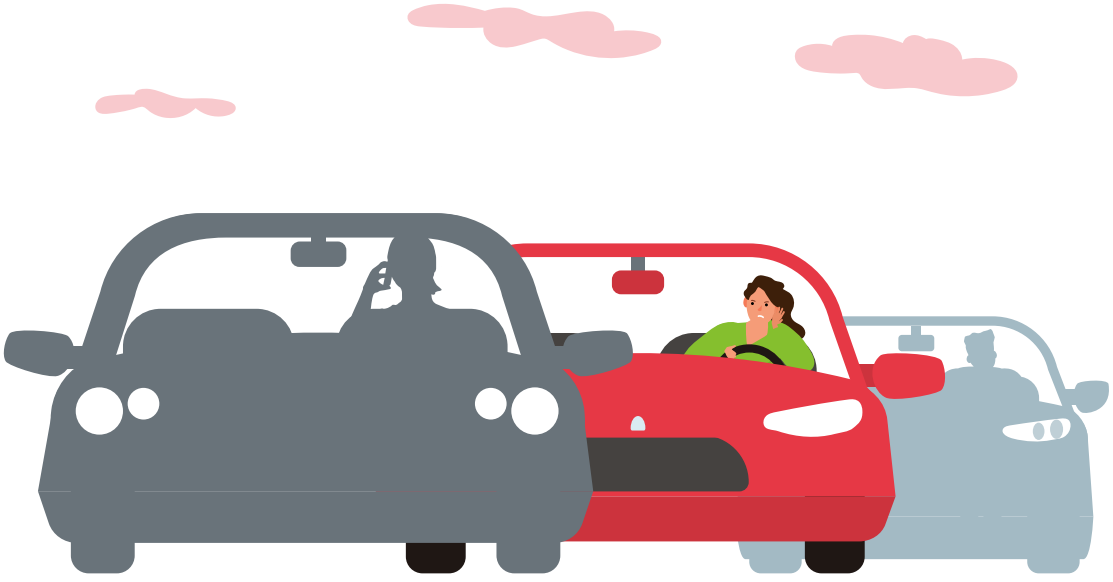
Margir hafa velt því fyrir sér af hverju DDoS árásir eru algengar ef þær eru í flestum tilvikum aðeins tímabundnar og hafa litlar sem engar langvarandi afleiðingar fyrir þann sem árásinni var beint að. Slíkar árásir eru ólíkar öðrum en oft getur það tekið töluverðan tíma og krafist mikillar vinnu að koma tölvukerfum aftur í sama horf og fyrir árás.

Þekktur hópur aðgerðasinna (NoName057) lýsti yfir ábyrgð á DDoS árásum sem framkvæmdar voru í tengslum við leiðtogafundinn á opinni Telegram-rás. Hann er þekktur stuðningshópur rússneskra stjórnvalda og hefur framið DDoS árásir víðsvegar þar sem umræðan er hliðholl Úkraínu.



Markmið árásanna er meðal annars að ergja almenning í von um að samstaða með Úkraínu minnki.

Aðrir hópar sem beita DDoS árásum láta ekki af þeim fyrr en lausnargjald hefur verið greitt. Einnig hefur DDoS árásum verið beitt sem tálbeitu þar sem þær eru þess eðlis að þær grípa athygli strax og vinna fer í gang við að reyna að stöðva árásina með ýmsum leiðum. Hópar hafa á meðan framið aðrar árásir eða komið sér inn í kerfi í skugga DDoS árásanna.



Þegar fjölmargir mæta í bílalúgu án þess að ætla sér að kaupa neitt lengja þeir biðina fyrir raunverulega neytendur og koma jafnvel í veg fyrir að þeir komist að.

Veikleikagreining

Árið 2023 voru hugbúnaðarveikleikar helsta ástæða árangursríkra netárása. Þeir veittu ógnaraðilum leiðir til að brjótast inn í kerfi, öðlast aukin réttindi og sniðganga öryggisvarnir. Samtals voru 26.447 veikleikar uppgötvaðir á síðasta ári; þar af höfðu 7.033 prófunarkóða (e. Proof of Concept – POC), en aðeins 206 þeirra voru nýttir í árásum.

Veikleikar 2023:

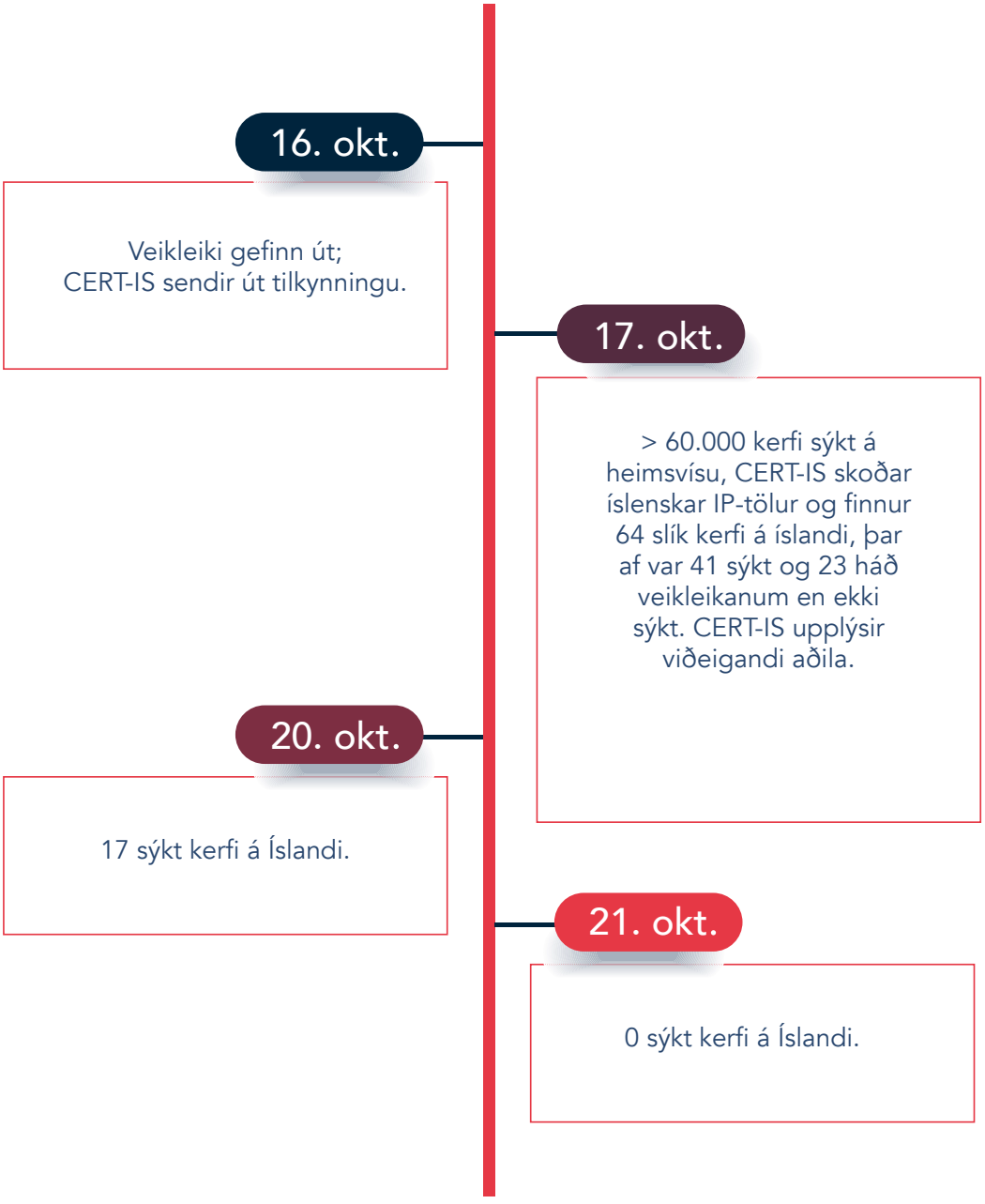
Að meðaltali líða 44 dagar frá því að veikleiki er opinberaður þar til hann er fyrst misnotaður. Hins vegar er 25% veikleika nýttur samdægurs eða jafnvel áður en veikleikarnir eru birtir opinberlega og 75% innan 19 daga. Þetta sýnir þörfina á fljótu viðbragði.

100%	26,5%	0,77%
Allir veikleikar	Veikleikar með prófunarkóða	Veikleikar nýttir í árásum
26.447	7.033	206

Alvarlegur CISCO veikleiki misnotaður hratt

Dæmi um hversu hratt ógnaraðilar geta nýtt sér veikleika er Cisco IOS XE veikleikinn (CVE-2023-20198) sem tilkynnt var um þann 16. október 2023. Veikleikinn var metinn með hámarks CVSSv3 skor upp á 10.0 og gerði óauðkenndum ógnaraðila kleift að búa til notendur á innbrotskerfum með hæstu réttindum og ná þar með stjórn á búnaðinum. Auðvelt var að misnota veikleikann og voru fleiri en 60.000 staðfest smit á heimsvísu aðeins einum degi eftir birtingu hans.

CERT-IS brást við, sendi út tilkynningar og leitaði að íslenskum IP-tölum sem keyrðu hugbúnaðinn. Greiningin leiddi í ljós að 64 slík kerfi voru sett upp á Íslandi og þar af hafði innbrot átt sér stað í 41 kerfi og hafði spillikóða verið komið fyrir þar. CERT-IS upplýsti rekstraraðila IP-talnanna og leiðbeindi þeim um hvernig hægt væri að hreinsa og uppfæra kerfin. Vel var tekið í ábendingarnar og aðeins fjórum dögum síðar voru engin sýkt kerfi eftir á Íslandi.



Þökk sé þessum aðgerðum var hægt að loka á árásaraðilana í öllum tilfellum og hlaust enginn frekari skaði af veikleikanum. Án slíkra viðbragða hefðu þessi innbrot mögulega verið upphafið að mun alvarlegri árásum, svo sem gagnastuldi eða gagnagíslatöku. Þetta dæmi sýnir mikilvægi þess að bregðast skjótt við veikleikatilkynningum til að viðhalda öryggi með reglulegum uppfærslum.

Þróun á vefveiðum

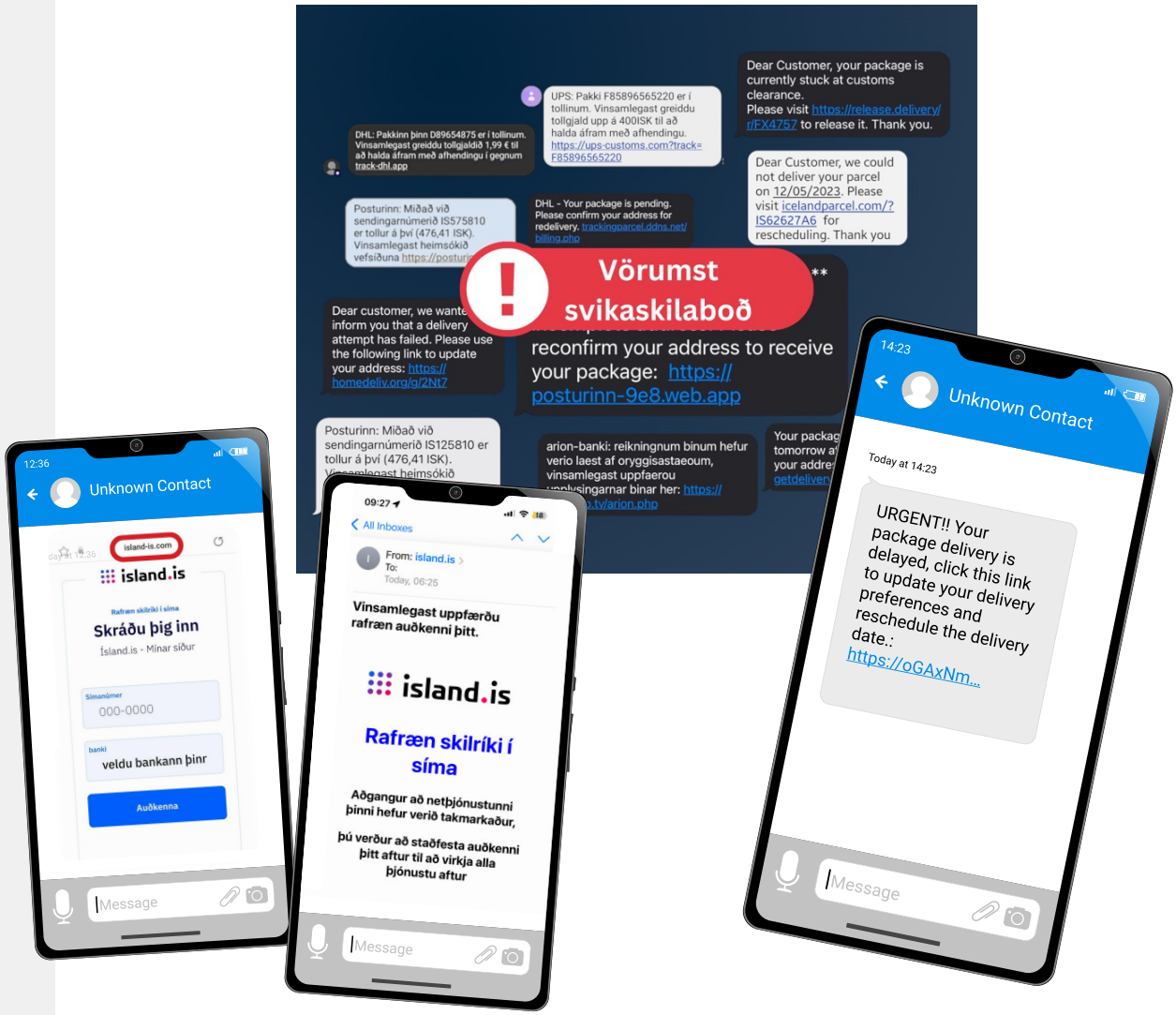
Líkt og undanfarin ár voru svik umfangsmesti flokkur netöryggisatvika á Íslandi árið 2023. Svikin eru fjölbreytt, sum augljós en önnur útsmogin og erfiðari að greina. Þau byrja í nær öllum tilfellum á einhvers konar skilaboðum; algengust eru SMS, skilaboð á samfélagsmiðlum eða vefpóstur. Við minnstu efasemdir er gott að hringja beint í þann sem sendir skilaboðin. Ef um fyrirtæki er að ræða skal nota símanúmer beint af heimasíðu þess, ekki úr skilaboðunum sjálfum.

Sumar af svikaherferðunum voru nýjar af nálinni og greinilegt að mikil undirbúningsvinna fór í að sníða herferðina að íslenskum kerfum. Í fyrsta skiptið voru island.is eftirlíkingar notaðar í svikaherferðum þar sem markmiðið var oftast að komast inn í heimabanka einstaklinga. Aðilum bárust skilaboð þar sem ýjað var að mikilvægu erindi og að þörf væri á innskráningu á island.is eins fljótt og hægt væri. Hélt fólk þá að það væri að skrá sig inn á island.is í raun voru árásaraðilarnir að nýta upplýsingarnar til að skrá sig inn í banka viðkomandi á bak við tjöldin. Seinna breyttust þessi svik þannig að fólk var beðið um að tilgreina viðskiptabanka sinn samhliða innskráningunni á island.is svikasíðuna. Gátu árásaraðilar þannig vitað í hvaða heimabanka þeir ættu að reyna innskráningu.

Mikill munur var á SMS svindlum milli ára og var íslenskan í svikaskilaboðunum oft það góð að fólk átti erfitt með að sjá að um svindl væri að ræða. Þóttust aðilarnir gjarnan vera á vegum banka viðtakanda og hótuðu að loka bankareikningum. Einnig þóttust svindlarar vera á vegum sendingaþjónustu og sögðu upplýsingar vanta til að koma pakka á leiðarenda. Í báðum tilvikunum hafði nánast fullkomin endurgerð þeirrar heimasíðu, sem fólk hélt að það væri að fara inn á, verið sett upp. Svindlararnir reyndu annað hvort að komast inn í heimabanka fólks með því að fá það til að samþykkja rafræna auðkenningu og/eða blekkja það til að gefa upp greiðslukortaupplýsingar.

Um mitt sumar 2023 kom holskefla af fyrirmælasvikum (e. Business Email Compromise) og vara þurfti sérstaklega við þeim. Voru skilaboðin á góðri íslensku svo fólki reyndist erfitt að sjá í gegnum þau. Sumarið er vinsæll tími fyrir fyrirmælasvik þar sem mörg fyrirtæki reiða sig á sumarstarfsmenn sem eru reynsluminni og er hættara við að fylgja leiðbeiningum án þess að skoða tölvupóstinn vandlega eða spyrjast fyrir um hvort beiðnin sé eðlileg.

Í fyrirmælasvindlum líkir árásaraðili með einum eða öðrum hætti eftir yfirmanni eða samstarfsaðila til að blekkja starfsfólk, oft til að greiða háar fjárhæðir, til árásaraðila í stað samstarfsaðila.



Gervigreind í netöryggi

Gervigreind skipaði stóran sess í umræðunni árið 2023 og setti svip sinn á fjölmörg svið. Spunagreind (e. generative AI) líkt og ChatGPT og DALL-E var þar áberandi en hún er fær um að skrifa ræður, útbúa tónlistarábreiður eða listaverk út frá lýsingum notandans á einungis nokkrum sekúndum. Það var því ekki að ástæðulausu að gervigreind var orð ársins hjá ýmsum stofnunum.

Því hefur verið velt upp hvaða áhrif þessi tækni mun hafa á upplýsingaöryggi. Þegar þetta er skrifað eru ekki til staðfest dæmi um óværur skrifaðar af gervigreind þó vísbendingar séu um það. Netárásir geta verið af ýmsum toga og vísbendingar um aðstoð gervigreindar má sjá í betur orðuðum vefveiðapóstum og því hversu hratt nýuppgötvaðir veikleikar í kerfum eru misnotaðir í ákveðnum tilfellum.

Eitt dæmi sem varpað hefur verið fram um hvernig árásarhópar gætu nýtt sér gervigreind er með samstarfi mismunandi mállíkana sem vinna að ákveðnu markmiði. Eitt þeirra gæti séð um skönnun eftir veikleikum á nettengdum kerfum, annað um úrvinnslu þeirra niðurstaðna og ákvörðun á árásarvinkli út frá þeim. Við þetta mætti svo lengi bæta en kjarni málsins er sá að möguleikarnir eru miklir.

Möguleikarnir einskorðast ekki við óprúttna aðila. Gervigreind getur einnig hjálpað til við netvarnir því getan til gagnasöfnunar, greiningar og úrvinnslu með þessari tækni er gríðarleg. Talið er að gervigreind eigi mikið inni en nú þegar jafnast geta hennar á við eða tekur fram úr sérfræðiþekkingu á ýmsum sviðum. Við þetta er að bæta að ýmsir birgjar í netöryggisbransanum eru byrjaðir að nýta sér gervigreind í einhverri mynd.

Spunagreind er gervigreind sem getur búið til texta, myndir eða önnur gögn, oft út frá skipunum eða lýsingum notandans.

Gervigreind í netöryggi

CERT·IS

ÁRSSKÝRSLA 2023

Augljóst er að gervigreind hefur skipað sér stóran sess í tækniumhverfinu okkar, sennilega um ókomna tíð. Framþróunin er mikil og mikilvægt að sofna ekki á verðinum heldur fylgjast vel með tækifærunum sem tæknin ber með sér og nýta þau til að efla netvarnir þegar ástæða er til.


CERT·IS