FRÉTTABLAÐIÐ

Rafrænt öryggi

KYNNINGARBLAÐ

FÖSTUDAGUR 28. janúar 2022

Kynningar: Síminn, Dokobit, Persónuvernd, Þekking, Resecurity, Advania.

María Böndal, deildarstjóri viðskiptatengsla, og Hlynur Guðmundsson, forstöðumaður fyrirtækjalausna Símans. MYND/KRISTINN BERNHARD

Öruggara net með Fyrirtækjapakka frá Símanum

Rafrænt öryggi skipti æ meira máli í rekstri fyrirtækja og stofnana. Síminn býður nú upp á Fyrirtækjapakka með netöryggi og öll fjarskipti fyrirtækisins í einum pakka.

Rafrænt öryggi skiptir mjög miklu máli í rekstri fyrirtækja og stofnana í dag. Starfsfólk Símans hefur séð mikinn vöxt undanfarin ár í beinum netárásum (DDOS) þar sem tilgangurinn er að lama þjónustur viðkomandi rekstraraðila með miklu magni fyrirspurna og ýmiss konar svindltilraunum til að hafa peninga út úr fyrirtækjum, segja þau Hlynur Guðmundsson, forstöðumaður fyrirtækjalausna, og María Blöndal, deildarstjóri viðskiptatengsla hjá Símanum. „Nú er svo komið að það er enginn óhultur og fjarlægð Íslands eða smæð virðist ekki fæla aðila frá því að sækja hingað eins og dæmin sanna," segir Hlynur. Oft eru þetta „drive by" árásir þar sem netið á Íslandi er skannað og leitað eftir þekktum veikleikum í fyrstu vörn fyrirtækja. „Aðferðirnar sem menn beita eru sífellt að þróast og tæknin hjálpar því miður í þessum efnum en íslenskan í svindlpósti er oft ansi góð þó að stundum séu áberandi villur sem ættu að vekja fólk til umhugsunar. Gagnagíslatökuárásir hafa einnig orðið algengari þar sem gögn fyrirtækja eru dulkóðuð og krafist lausnargjalds til að endurheimta þau," bætir María við.

Einn eldveggur ekki nóg

Að þeirra sögn dugar ekki lengur að setja upp einn eldvegg og halda að þar með sé hægt að haka í eitthvert box við rafrænt öryggi. „Eldveggurinn þarf að vera það sem kallað er næstu kynslóðar eldveggur og meðvitaður um miklu meira en bara IP-tölur og gáttir og vera »

> **Nú er svo komið að enginn er óhultur og fjarlægð Íslands eða smæð virðist ekki fæla menn frá því að sækja hingað.**
>
> Hlynur Guðmundsson

» undir stöðugri vöktun. Að auki þurfa fyrirtæki að gera ráð fyrir að það sé alltaf einhver leið fram hjá fyrstu vörnum. Vakta þarf alla netumferð á innra neti fyrirtækja og geta þannig gripið inn í þegar óværan er komin inn fyrir fyrstu varnir en oft líður töluverður tími frá því að glæpamenn komast inn í fyrirtækin áður en þeir láta loks til skarar skríða," segir Hlynur.

Lítil og meðalstór fyrirtæki á Íslandi eru ekki undanskilin þessari hættu frekar en einstaklingar. „Öll erum við tengd við netið á einn eða annan hátt og þannig erum við öll gerð að skotmörkum," segir María.

Hentug lausn

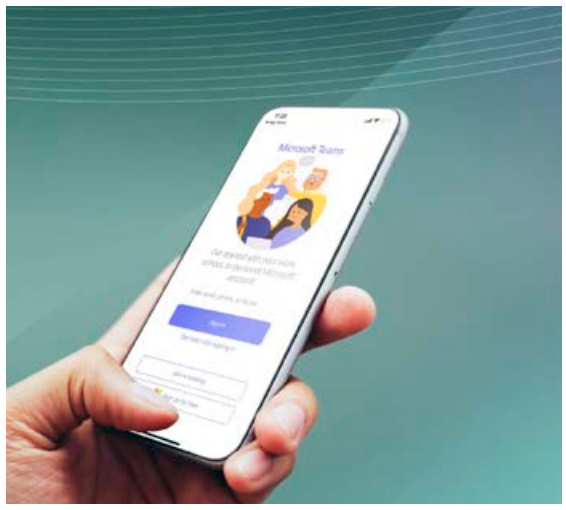
Síminn býður fyrirtækjum upp á Fyrirtækjapakka með netöryggi og öll fjarskipti fyrirtækisins í einum pakka. Í því felst bæði mikið hagræði og öryggi fyrir viðskiptavini að þeirra sögn. „Hingað til hefur verið kostnaðarsamt og flókið að setja upp góðar rafrænar varnir og halda þeim við. Í raun hefur það aðeins verið á færi stærri fyrirtækja að reka slíkar lausnir með réttum hætti," segir María. „Við sáum tækifæri í því að bjóða fyrirtækjum hagkvæma lausn sem færir þeim hágæða öryggislausnir frá Fortinet sem er leiðandi fyrirtæki í netöryggi í heiminum í dag og byggja allar sínar lausnir á miðlægri stýringu með yfirsýn yfir allt sem er í gangi á innra neti fyrirtækja."

Sérfræðingar Símans sjá svo um að reka og uppfæra búnaðinn ásamt því að vakta hann og upplýsa viðskiptavininn um leið og ástæða er til segir Hlynur. „Þannig er til dæmis hægt að sjá ef vél sýkist af óværu, útiloka hana frá öðrum vélum og bregðast hratt og örugglega við. Að auki er innifalið netsamband með ótakmörkuðu gagnamagni ásamt varaleið sem tryggir hámarks uppitíma ef eitthvað kemur upp á. Lausnin innifelur næstu kynslóðar eldvegg og fyrsta flokks búnað fyrir þráðlaust net sem tryggir hámarks upplifun innan hvers vinnustaðar. Þannig getum við til dæmis brugðist við dreifðum álagsárásum og minnkað þann skaða sem þær annars gætu unnið á rekstri fyrirtækja."

Hægt er að bæta við ýmsum aukaþjónustum enda þarfir fyrirtækja misjafnar, að þeirra sögn. Sem dæmi er hægt að bæta við endalausri 5G-farsímaáskrift fyrir 3.000 krónur.

Nýju áskriftirnar eru á föstu mánaðargjaldi sem eru á færi allra fyrirtækja. Stærri fyrirtæki geta fengið sérsniðnar lausnir, til dæmis þegar tengja þarf saman nokkur útibú og flækjustigið verður meira.

Síminn vinnur að uppbyggingu fimmtu kynslóðar farsímakerfa með búnaði frá Ericsson. MYNDIR/SÍMINN



Það er mjög auðvelt að bæta lausnum við fyrirtækjapakka líkt og Microsoft Teams eða Webex.

Mannfólkið er oft veikasti hlekkurinn þegar kemur að hættum í tengslum við rafrænt öryggi.

> **Öll erum við tengd við netið á einn eða annan hátt og þannig erum við öll gerð að skotmörkum.**
>
> María Blöndal

Mannfólk veikasti hlekkurinn

Þau eru sammála um að þegar kemur að hættum í tengslum við rafrænt öryggi sé mannfólkið oftast veikasti hlekkurinn. „Auðveldasta leiðin fyrir óprúttna aðila er að plata okkur í gegnum tölvupósta og skilaboð og fá okkur til dæmis til að smella á hlekk sem opnar á óværu sem er hönnuð til að komast inn fyrir varnir fyrirtækja," segir Hlynur. Aðrar þekktar leiðir eru í gegnum veikleika, óuppfærðan hugbúnað eða hreinlega hugbúnað og tæki sem eru vitlaust uppsett. „Það sem var öruggt í gær þarf ekki að vera öruggt í dag. Þetta er endalaus eltingarleikur sem þarf að sinna af alvöru. Þess vegna er til dæmis mikilvægt að hafa yfirsýn yfir allan hugbúnað sem er í notkun á tölvum starfsfólks og uppfæra hann reglulega því þessir óprúttnu aðilar eru fljótir að finna veikleika og nýta sér þá," segir María.

Aðeins fyrsta skref

Þau segja Fyrirtækjapakkann vera aðeins fyrsta skref af mörgum þegar kemur að netöryggi viðskiptavina Símans. „Varnir fyrir búnað notenda utan vinnustaðar og afritun gagna er til dæmis eitthvað sem þarf að hafa í huga. Fyrirtæki á Íslandi munu þurfa að setja aukna athygli á netöryggi því í verstu tilfellum getur það orðið svo að það kemst með illum leik aftur á lappirnar," segir María. Fréttum af netárásum á fyrirtæki á Íslandi mun fjölga ef ekkert er að gert, bætir Hlynur við. „Netárásir eru ekki einkamál kerfisstjóra og sérfræðinga í upplýsingatækni heldur alls starfsfólks. Ein misráðin ákvörðun eða mistök gerð í flýti geta haft keðjuverkandi áhrif sem gætu haft mjög alvarleg áhrif á vinnustaðinn," bætir Hlynur við. „Því þarf að bregðast við fyrr en seinna og koma þessum málum í betra horf hjá flestum ef ekki öllum fyrirtækjum og stofnunum í landinu, uppfæra og vakta öll þessi kerfi og halda vörnum uppi allan sólarhringinn." ■

Nánar á siminn.is.

Útgefandi: Torg ehf | **Ábyrgðarmaður:** Björn Víglundsson | **Sölumaður auglýsinga:** **Arnar Magnússon,** arnarm@frettabladid.is, s. 550 5652. | **Veffang:** frettabladid.is

Ragna Klara Magnúsdóttir, viðskiptastjóri Dokobit á Íslandi. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

Ný fullgild rafræn skilríki fyrir alla í Evrópu

Fyrirtækið Dokobit sem þróar lausnir fyrir rafrænar undirskriftir og aðrar traustþjónustur er í miklum vexti í Evrópu. Fyrir skömmu studdi Dokobit rafræn skilríki frá 14 löndum en hefja nú dreifingu á nýjum rafrænum skilríkjum sem standa öllum til boða í Evrópu.

„Fyrirtækið Dokobit býður upp á rafrænar undirskriftir og lausnir fyrir rafræna auðkenningu. Dokobit var stofnað árið 2008 og er því komið með góða reynslu í stafræna geiranum, en í grunninn er þetta litáískt fyrirtæki sem var stofnað af tveimur félögum," segir Ragna Klara Magnúsdóttir, viðskiptastjóri Dokobit á Íslandi. „Þetta hefur verið í eigu þeirra þar til nú í ágúst, þegar fyrirtækið sameinaðist norska fyrirtækinu Signicat, sem hefur verið í gríðarlegum vexti undanfarin ár. Það hefur keypt fimm fyrirtæki að undanförnu, þar af þrjú bara á síðasta ári."

Gríðarlegur vöxtur í rafrænum undirskriftum

„Signicat er komið með skrifstofur um alla Evrópu og stefnir á að verða stærst í Evrópu fyrir rafrænar undirskriftir og auðkenningar. Þau sáu Dokobit sem mjög sterkan aðila og mikil tækifæri við að sameina krafta fyrirtækjanna," segir Ragna. „Sameiningin hefur gengið ótrúlega vel, við smullum bara saman eins og hönd í hanska og við vorum með ýmsar lausnir sem þau voru komin styttra með.

Þessi sameining hefur styrkt okkur mjög mikið og gert okkur kleift að vaxa ennþá hraðar. Stefnan er nú að auka starfsmannafjöldann um 70 manns bara á þessu ári, en til samanburðar var Dokobit með 32 starfsmenn í heild fyrir ári síðan en ef við teljum Signicat með erum við í dag 440 manns," segir Ragna.

Ný rafræn skilríki

„Fyrirtæki í eigu Signicat gefur út fullgild rafræn skilríki og sérhæfir sig í að auðkenna einstaklinga með svokölluðu „video onboarding" ferli, en það þýðir að fólk getur fengið ný rafræn skilríki afhent með því að nota vefmyndavél og vegabréf eða önnur persónuskilríki til þess að fá ný fullgild rafræn skilríki," segir Ragna. „Þetta afhendingarferli er eIDAS-vottað, sem þýðir að þessi skilríki eru í hæsta gæðaflokki þegar kemur að útgáfu rafrænna skilríkja.

Þessi skilríki gera það að verkum að íslenskt fyrirtæki getur sent skjal til undirritunar hvert sem er í Evrópu og fengið fullgilda rafræna undirskrift. Þetta þýðir að við getum núna boðið þjónusturnar okkar í allri Evrópu án þess að fórna gæðum með að því nota lægri stig af rafrænum undirskriftum.

Við stefnum að því að geta boðið stærri fjármálafyrirtækjum mjög öruggar og áreiðanlegar lausnir, en meðal viðskiptavina Signicat eru stórfyrirtæki eins og Facebook, Paypal, American Express, Mastercard, Volvo og fleiri. Þetta er allt annað en við vorum vön fyrir ári síðan," segir Ragna. „Hér heima höfum við samt einnig verið að sinna mjög stórum fyrirtækjum. Íslandsbanki, Vodafone, Samgöngustofa, fasteignasölur og stærri bílaumboð eins og BL og Toyota eru í viðskiptum hjá okkur, sem og önnur fyrirtæki í fjármálastarfsemi og ríkisstofnanir.

Þessi stærri fyrirtæki eru okkar aðalkúnnahópur, en við erum líka að þjónusta fjölmarga einyrkja og minni fyrirtæki, enda er hugsjónin sú að rafrænar undirskriftir séu fyrir alla," segir Ragna.

> **Þessi skilríki gera það að verkum að íslenskt fyrirtæki getur sent skjal til undirritunar hvert sem er í Evrópu og fengið fullgilda rafræna undirskrift.**
>
> Ragna Klara Magnúsdóttir

Einfalt að nýta þjónustuna

„Við erum með mjög marga sterka samstarfsaðila í rafrænum undirskriftalausnum og viljum nefna Origo, Arango, Sensa, Hugvit, Spekta, Ozio, Rögg, ThinkSoftware, Wise og mörg fleiri," segir Ragna. „Við erum því í samstarfi við öll helstu hugbúnaðarhúsin og þau hafa gert margar innleiðingar á okkar þjónustum, þannig að fyrir aðila sem kaupa lausnir frá þessum aðilum er mjög einfalt að virkja rafrænar undirskriftir beint úr kerfunum.

Fyrir fyrirtæki sem eru að nota Microsoft-lausnir er þetta til dæmis lítið og einfalt stökk, það þarf bara að hafa samband og óska eftir að þetta sé tengt," segir Ragna. „Þar sem samtengingin er tilbúin á Microsoft Marketplace er hægt að byrja að nota rafrænar undirskriftir í sömu viku."

Sterk rafræn auðkenning

„Dokobit er einnig með lausnir fyrir auðkenningar með rafrænum skilríkjum eins og við þekkjum öll úr heimabönkum, island.is og Heilsuveru. Lausnin styður rafræn skilríki í farsímum, kortum eða með Auðkennisappinu sem eru ný rafræn skilríki frá Auðkenni," segi Ragna. „Auðkennisappið hefur þann kost fram yfir skilríki á farsíma að notandinn þarf ekki lengur að vera með íslenskt símanúmer til þess að nota skilríkin. Þetta kemur sér til dæmis mjög vel fyrir Íslendinga sem eru búsettir eða í námi erlendis.

Auðkenningarlausnin er svokölluð „plug-in" lausn, þannig að hvaða fyrirtæki sem er getur bara tengt þetta inn á sína heimasíðu og sett upp rafræna auðkenningu á sína síðu fyrir innskráningar, netverslun eða hvað sem er," segir Ragna. „Viðskiptavinir geta einnig aðlagað útlitið á innskráningarglugganum þannig að það falli fullkomlega inn í þeirra eigið viðmót. Á sama tíma og verslun og þjónusta er í auknum mæli að færast yfir á netið er enn mikilvægara að geta tryggt á öruggan hátt hverjum maður er að veita upplýsingar eða þjónustu."

Gerðu nýskráningu ökutækja rafræna

„Við vorum að klára verkefni með Arango í samvinnu við Samgöngustofu sem fól í sér að gera nýskráningar á ökutækjum 100% rafrænar. Ef þú ferð að kaupa nýjan bíl núna hjá BL, Heklu eða Öskju geturðu fengið bílinn um fimm dögum fyrr en áður, að meðaltali, eftir að þetta breyttist. Þannig að nú getur þú fengið bílinn afhentan nánast samdægurs," segir Ragna.

„Áður var starfsmaður í vinnu við að keyra með gögn á milli aðila og safna undirskriftum úr hinni og þessari átt áður en öllum gögnunum var skilað til Samgöngustofu og þar var síðan allt handslegið inn," útskýrir Ragna. „Það er því gríðarleg hagræðing í því að gera þessa skráningu rafræna og fólk sem starfar í bílageiranum hefur verið rosalega ánægt með þessa breytingu."

Lækkuð verð

Dokobit lækkaði þjónustugjöld á síðasta ári vegna þess að það hefur verið svo mikil aukning í fjölda notenda.

„Aukningin hjá okkur var yfir 400% á síðasta ári og viðskiptavinahópurinn hefur þrefaldast á einu ári, svo við ákváðum að lækka verðin okkar," segir Ragna. „Rafrænar undirskriftir eiga ekki að vera dýr tækni þannig að verð spili hlutverk í hvort fyrirtæki noti þær heldur sjálfsögð tækni sem fyrirtæki geta nýtt til þess að veita viðskiptavinum bestu þjónustu sem völ er á. Við reynum stöðugt að lækka verðin okkar til þess að styðja við þessa framtíðarsýn sem við getum gert með aukinni notkun," segir Ragna. „Það hefur líka verið raunin, viðskiptavinir hafa verið tryggir og líkað mjög vel hversu áreiðanlegar lausnirnar okkar eru og erum við að sjálfsögðu mjög þakklát góðum og traustum hópi ánægðra viðskiptavina." ■

Electronic IDentification

Signicat

Of veik lykilorð eru ein helsta hættan á netinu

Netöryggi og öryggi viðkvæmra og dýrmætra gagna er fólki ofarlega í huga í upphafi rafrænnar aldar. Tækninni fleygir fram og notendur eiga fullt í fangi með að fylgjast með því sem er að gerast. Margar hættur þarf að varast.

olafur@frettabladid.is

Andri Heiðar Kristinsson, framkvæmdastjóri Stafræns Íslands, segir helstu mistök netnotenda varðandi öryggi á netinu felast í veikum lykilorðum. FRÉTTABLAÐIÐ/ANTON BRINK

Við tókum hús á Andra Heiðari Kristinssyni, framkvæmdastjóra Stafræns Íslands, og báðum hann að fara aðeins yfir nokkur mikilvæg atriði varðandi rafrænt öryggi.

Hversu örugg eru okkar viðkvæmustu gögn sem við erum með í tölvunum okkar og símum, eins og til dæmis bankaupplýsingar, lykilorð, ljósmyndir og þess háttar?

„Almennt þá eru gögnin okkar nokkuð örugg ef við göngum vel um og erum meðvituð – en líkt og með heimili okkar þá geta óprúttnir aðilar því miður stundum brotist inn með einbeittum brotavilja. Þess vegna er gott að læsa og jafnvel fá sér öryggiskerfi. Nettengdu tækin okkar eru ekki ósvipuð og mikilvægt að við séum upplýst um hvað við erum að vista hvar. Lykilorð er til að mynda öruggast að geyma í stafrænum „lyklakippum“ eða öruggum lykilorðageymslum. Heimabankarnir okkar eru til dæmis með sterk öryggiskerfi þar sem við komumst aðeins inn með okkar auðkenni eða rafrænum skilríkjum.“

Á almannafæri á netinu

Andri Heiðar segir gott að hafa ákveðin atriði í huga varðandi netöryggi. „Númer eitt myndi ég setja að vera upplýstur um hvar þú ert nettengdur, hvað beri að varast og muna að þú ert á almannafæri þegar þú ert á netinu. Rétt eins og í raunheimum ertu almennt öruggari í bankanum þínum eða inni á lögreglustöð. Þannig að hvar þú ert og hvað þú ert að gera skiptir máli.“

> **Rafræn ógn hefur aukist upp á síðkastið samhliða þeim hröðu tæknibreytingum sem orðið hafa í heiminum.**

Klassísk ráðlegging snýr líka að lykilorðum en mikilvægt er að nota flókin lykilorð og geyma í rafrænni „lyklakippu“. „Með því bætist við það öryggi að rafræna lyklakippan áttar sig á ef til dæmis er um að ræða hakkara að þykjast vera heimabankinn þinn. Það er einnig mikilvægt að velja sér lykilorð sem ekki eru of augljós á borð við afmælisdaga eða nöfn nánustu fjölskyldumeðlima – en slíkt er alltof algengt! Staðreyndin er sú að algengasta lykilorðið í heiminum er „123456“ og að velja slíkt lykilorð er álíka sniðugt og að skilja eftir galopna hurð á heimilinu þegar farið er í frí,“ segir Andri Heiðar.

En hver skyldu vera helstu mistökin sem fólk gerir varðandi rafrænt öryggi?

Að sögn Andra Heiðars felast algengustu mistökin líklega í of veikum lykilorðum. Þar á eftir komi líklega „óþolinmæðin“ sem endurspeglist í því að við samþykkjum allt án athugunar því að við séum að flýta okkur. „Það getur kostað okkur óþarfa eltihrella. Í því samhengi má nefna að varast ber að smella á hlekki eða opna viðhengi í tölvupósti ef einhverjar grunsemdir vakna, svo sem ef þú þekkir ekki lénið sem tengillinn vísar á eða ef íslenskan (tungumálið) er mjög bjöguð eða ef þú kannast ekki við sendandann. Ef einhver vafi er um slíkt er betra að kanna málið áður en haldið er áfram. Flest rafræn innbrot í dag eiga uppruna sinn í einföldum mistökum notenda sem hægt er að koma í veg fyrir með fræðslu og þjálfun.“

Fjarvinna eykur ekki hættuna

Skyldi hætta vera fólgin í því fyrir netöryggi heimilisins eða fyrirtækisins þegar fólk tengist tölvukerfi í vinnunni úr sinni einkatölvu eða úr vinnutölvu sem tengd er við þráðlaust net heimilisins?

Flest fyrirtæki sem bjóða upp á fjarvinnu hafa að sögn Andra Heiðars styrkt netöryggið – eða ættu að hafa gert slíkt. Almennt séð sé ekki mikil hætta á innbroti af þessum sökum, samanborið við ofangreind atriði, ef öryggi tölvukerfa á vinnustaðnum er fullnægjandi. Mikilvægt sé þó að vera ekki á opnu neti með efni sem krefst mikils gagnaöryggis. „Öll heimanet ættu að minnsta kosti að hafa lykilorð og vera ekki öllum opin en ég hvet alla þá sem eru í fjarvinnu að fara yfir þessi mál með sínum vinnuveitanda.“

Er það rétt sem maður hefur á tilfinningunni að rafræn ógn hafi aukist upp á síðkastið?

„Já, það má með sanni segja það að rafræn ógn hafi aukist upp á síðkastið samhliða þeim hröðu tæknibreytingum sem orðið hafa í heiminum. Hakkarar virðast vera að færa sig upp á skaftið og innbrotum hefur fjölgað talsvert, en að sama skapi er vitundarvakning fólks að aukast og það er lykilatriði.

Þessu má kannski líkja við það að fyrir nokkrum áratugum þótti ekki sjálfsagt að nota bílbelti í bíl, en fæstum okkar dytti í hug að sleppa því í dag vegna aukinnar vitundarvakningar. Það nákvæmlega sama er uppi á teningnum í sambandi við netöryggi, við þurfum að kynna okkur mikilvægustu öryggisatriðin og vera meðvituð um að haga okkur eftir aðstæðum.

Að lokum vil ég nefna að netöryggi og persónuvernd er fólki eðlilega ofarlega í huga þessa dagana enda fleygir tækninni fram og við sem nýtum hana eigum fullt í fangi með að halda í við hana. Öryggi allra þeirra umsókna og lausna sem hið opinbera þróar er afar mikilvægt og ekki nóg að almenningur bæti sína meðvitund heldur þurfa fyrirtæki og stofnanir oft að taka sig betur á, eins og ýmis nýleg dæmi sýna. Almenningur á að geta treyst því að hið opinbera sé að gæta hagsmuna hans en að sama skapi þarf fólk sjálft að hafa augun opin,“ segir Andri Heiðar Kristinsson, framkvæmdastjóri Stafræns Íslands. ■

Alþjóðlegur persónuverndardagur er í dag

Alþjóðlegi persónuverndardagurinn er haldinn hátíðlegur í dag og verður ýmislegt í gangi af því tilefni. Meðal annars mun Persónuvernd, í samstarfi við Embætti landlæknis og Stafrænt Ísland, kynna fyrirhugað tilraunaverkefni sem nefnist sandkassaverkefni.

> **Persónuvernd snýst í grunninn um að tryggja stjórnarskrárvarin réttindi einstaklinga til einkalífs.**

Vigdís Eva Líndal starfar hjá Persónuvernd og heldur upp á daginn ásamt samstarfsfólki. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

Vigdís Eva Líndal, sviðsstjóri erlends samstarfs og fræðslu hjá Persónuvernd, segir daginn mikilvægan. „Persónuvernd snýst í grunninn um að tryggja stjórnarskrárvarin réttindi einstaklinga til einkalífs. Í dag verður tilkynnt um svokallað sandkassaverkefni eða sandboxing eins og það kallast á ensku. Verkefnið mun bjóða fyrirtækjum sem vilja þróa gervigreindarlausnir fyrir heilbrigðisþjónustu sérstakt samstarf við Persónuvernd, Embætti landlæknis og Stafrænt Ísland. Persónuverndardagurinn er haldinn hátíðlegur í dag víða um heim og er mikilvægur fyrir þær sakir að Evrópuráðssamningur var samþykktur þennan dag árið 1981. Samningurinn var fyrsta skrefið í að setja persónuverndarlög í Evrópu. Í nútíma rafrænu samfélagi hefur löggjöf um persónuvernd orðið enn mikilvægari. Það er mun auðveldara en áður að safna upplýsingum og vinna með þær, greina einstaklinga og fylgjast með því sem við erum að gera á netinu,“ útskýrir Vigdís Eva.

„Upphaflega var samningurinn gerður meðal annars vegna upplýsingaöflunar í síðari heimsstyrjöldinni og fólk flokkað í hópa eftir uppruna. Sömuleiðis kom í ljós mikil upplýsingasöfnun við hrun Berlínarmúrsins en Stasi var með um 90 þúsund starfsmenn í upplýsingaöflun og skrásetningu fólks. Miklar breytingar hafa orðið með tilkomu tölvutækninnar sem hefur gert fyrirtækjum og stjórnvöldum kleift að safna og vinna með sífellt meira af upplýsingum. Þess vegna voru einnig sett ný evrópsk persónuverndarlög árið 2018, GDPR, til að mæta þessari rafrænu þróun. Síðastliðin ár hafa mörg gagnafyrirtæki, til dæmis samfélagsmiðlar, komið fram á sjónarsviðið en þeirra helsta tekjulind er að safna og vinna með persónuupplýsingar,“ segir Vigdís Eva.

„Við hjá Persónuvernd reynum alltaf að gera eitthvað á hverju ári til að fagna deginum. Í dag munum við kynna sandkassaverkefnið okkar en það er tilraunaverkefni að norskri og breskri fyrirmynd. Við munum bjóða fyrirtækjum sem eru að vinna gervigreindarlausnir fyrir heilbrigðisþjónustu að taka þátt í sandkassanum. Þar fá þau ákveðið rými undir okkar eftirliti til að þróa vöru sem uppfyllir skilyrði persónuverndarlaga og hefur mikið samfélagslegt gildi. Þessu mun ljúka með leiðbeiningum til annarra fyrirtækja sem eru að vinna með gervigreind í heilbrigðisþjónustu. Tilgangurinn er að finna lausnir á þeim persónuverndaráskorunum sem þessi fyrirtæki standa almennt fyrir og hvernig er best að leysa úr þeim. Vinnsla persónuupplýsinga með notkun ýmiss konar heilbrigðislausna hefur verið í brennidepli undanfarin ár, en með þeim er oft verið að vinna viðkvæmustu upplýsingarnar um okkur og nauðsynlegt að öryggið sé í lagi.“

Vigdís segir að það sé flókið og viðamikið starf að halda persónuverndarmálum í lagi. „Það er enginn dagur eins hjá okkur og verkefnin fjölbreytt. Lögin eru sérstök þar sem þau taka til stjórnvalda, fyrirtækja, frjálsra félagasamtaka, sveitarfélaga og fleiri,“ segir hún.

„Gagnsæi og sjálfsákvörðunarréttur eru tvö meginmarkmið persónuverndarlaga. Í því felst fyrst og fremst að þeir sem ætla að vinna með persónuupplýsingar verða að segja einstaklingnum hvaða upplýsingar þeir ætla að vinna með og hvers vegna, á skýru og einföldu máli. Auk þess þarf að vera heimild til að vinna upplýsingarnar, til dæmis á grundvelli samþykkis, samnings eða laga,“ greinir Vigdís frá og bætir við að sem betur fer hafi orðið vakning í því að fólk sé með öryggi og varnir í lagi. Undir tíu fyrirtækjum hafa fengið á sig sektir á síðustu fjórum árum fyrir brot á persónuverndarlögum. ■

Þjónustufyrirtækið Þekking veit mikilvægi þess að gæta öryggis á öllum sviðum upplýsingatækni. Þekking býður upp á sérsniðnar lausnir í rafrænum öryggismálum fyrir fyrirtæki og stofnanir af öllum stærðum og gerðum.

Þekking er þjónustufyrirtæki á sviði upplýsingatækni. Fyrirtækið var stofnað árið 1999 og er með starfsstöðvar á tveimur stöðum á landinu. Annars vegar á Akureyri og hins vegar í Kópavogi. Sérsvið Þekkingar er rekstrarþjónusta og ráðgjöf á sviði upplýsingatækni. Áslaug Dagbjört Benónýsdóttir starfar sem upplýsingaöryggisstjóri hjá fyrirtækinu. „Ég veiti einnig viðskiptavinum ráðgjöf um málefni sem tengjast upplýsingaöryggi og persónuvernd. Þjónusta okkar fer að mestu leyti fram á netinu. Í sumum tilfellum þarf að mæta á staðinn, en það fer allt eftir þörf hvers fyrirtækis fyrir sig," segir Áslaug.

Af skrifborðinu yfir í tölvuna

Starfsumhverfi fyrirtækja hefur í dag að stórum hluta færst af skrifborðinu og yfir í tölvuna. Það verður því æ mikilvægara fyrir fyrirtæki og stofnanir að fjárfesta í rafrænu öryggi. „Það muna margir eftir því hvernig skrifstofur voru hér fyrir tæplega 20 árum, þegar það sást ekki í sum skrifborð fyrir pappírum. Þá fólst öryggið í raun í því að læsa skrifstofunni og öryggiskerfi urðu æ algengari. Í dag fer vinnan að mestu leyti fram í tölvunni og minna er um útprentuð gögn, meðal annars þegar kemur að afhendingu gagna á milli notenda. Nú skiptir því öllu máli að huga að öryggginu í tölvunni."

Öryggi í fjarvinnu

Í faraldrinum hefur vinnuumhverfi margra fyrirtækja enn fremur breyst hratt og mikið. „Mörg störf sem áður voru unnin á skrifstofunni hafa færst inn á heimili fólks. Þessi breyting felur í sér aukið mikilvægi í því að skoða mögulegar áhættur sem tengjast því. Í því samhengi má meðal annars nefna nettengingar, aðgengi að tölvu og öryggisvitund starfsfólks. Vinnuumhverfi starfsfólks í fjarvinnu er ekki það sama og er á skrifstofunni. Því þarf að tryggja að öryggi upplýsinga sé ekki minna þegar unnið er í fjarvinnu en þegar unnið er á skrifstofunni. Með aukinni fjarvinnu má gera ráð fyrir því að netglæpamenn endurskoði einnig sínar starfsvenjur og umhverfi, og fari í auknum mæli að herja á starfsfólk og þau tæki sem það notar við fjarvinnu. Það er því mikilvægt að bregðast við síbreytilegum netöryggisógnum með forvörnum og tryggja öryggi í tíma."

Kortlagning

Viðskiptavinir Þekkingar eru fyrirtæki og stofnanir af ýmsum stærðum og gerðum. Að sögn Áslaugar er alltaf góð byrjun að taka stöðuna á öryggismálunum í fyrirtækinu. „Þá er hægt að meta betur hvar þarf að gera bragarbót á. Einnig er gagnlegt að fyrirtæki bæti við fræðslu um upplýsingaöryggi sem einum lið í fræðsluáætlun sína. Það að veita reglulega fræðslu um þær netógnir sem eru í gangi hverju sinni getur komið í veg fyrir gríðarlegt tjón ef til netárásar kemur.

Þegar kemur að því að huga að rafrænu öryggi í fyrirtæki eða stofnun skiptir máli að kortleggja fyrst stöðuna með tilliti til mikilvægis og viðkvæmni þeirra upplýsinga sem fyrirtækið eða stofnunin er að meðhöndla. Í því tilfelli að netárás skyldi eiga sér stað, þá þarf að spyrja sig gagnrýnna spurninga eins og: „Hvers getur starfsemin

Áslaug Dagbjört segir það mikilvægt að bregðast við síbreytilegum netöryggisógnum með forvörnum og tryggja öryggi í tíma.

MYND/HÁKON DAVÍÐ BJÖRNSSON

Mikilvægt að þekkja hætturnar

> Öryggisvitundarþjálfun verður sífellt mikilvægari eftir því sem netógnir aukast og ætti slík þjálfun í raun að vera hluti af menningu flestra fyrirtækja sem vinna með tölvur.
>
> Áslaug Dagbjört

verið án og hvers ekki?" Þannig er best að forgangsraða og verja gögnin og kerfin miðað við það."

Þekking býður upp á ýmsar lausnir er snúa að öryggismálum. „Það fyrsta sem við gerum er að þarfagreina umhverfi fyrirtækja og stofnana. Með því fáum við betri sýn á hvaða lausnir henta hverjum viðskiptavini fyrir sig. Öryggislausnir Þekkingar greina og bregðast við netógnum fyrirtækja og stofnana allan sólarhringinn allt árið um kring á öruggan og hagkvæman hátt. Sem dæmi má nefna að við bjóðum upp á lausnir sem veita öryggi í skýjalausnum og á útstöðvum sem og eftirlit á netumhverfi fyrirtækja þar sem við setjum upp svokallaða skynjara. Lausnirnar fela í sér sjálfvirka greiningu á öryggisatvikum á öllu neti fyrirtækis. Auk þess eru viðeigandi aðgerðir framkvæmdar í rauntíma bæði sjálfvirkt og af öryggissérfræðingum á okkar vegum. Sjálfvirkni öryggislausnanna gerir okkur kleift að verja öll mikilvæg tæki og gögn í umhverfi fyrirtækja."

Forvarnir felast í fræðslu

Þegar kemur að rafrænu umhverfi fyrirtækja og stofnana, þá er ýmislegt hægt að gera til þess að koma í veg fyrir rafrænar ógnir. „Það má fyrirbyggja með ýmsum hætti og vera eins vel varinn og hægt er. Það skiptir þá mestu máli að meta stöðugt umhverfið sitt með tilliti til þeirra ógna sem eru í gangi hverju sinni og fræða notendur. Það skiptir því lykilmáli að byrja á réttum stað, setja reglur, fræða starfsfólkið um meðhöndlun gagna og innleiða réttu varnirnar."

Þekking býður fyrirtækjum og stofnunum upp á námskeið í netöryggisvitund. „Öryggisvitundarþjálfun verður sífellt mikilvægari eftir því sem netógnir aukast og ætti slík þjálfun í raun að vera hluti af menningu flestra fyrirtækja sem vinna með tölvur. Þekking er í samstarfi við netöryggisfyrirtækið AwareGo varðandi þjálfun í netöryggisvitund. Um er að ræða stutt og skemmtileg myndbönd sem notendur fá send til sín í pósti vikulega eða mánaðarlega, allt eftir þörfum fyrirtækisins. Við aðstoðum fyrirtæki við að stilla upp áætlun er varðar netöryggisfræðslu starfsfólks. Þá taka fyrirtæki til dæmis ákvörðun um að byrja með fræðslu í þrjá til fjóra mánuði og taka svo stöðuna og meta þörfina, og ákveða þá hverjar áherslurnar ættu að vera í næstu þjálfun." ■

Vilja auka netöryggi á Norðurlöndunum

Bandaríska netöryggisfyrirtækið Resecurity hefur hafið samstarf við íslenska fyrirtækið SecureIT með það að markmiði að auka netöryggi á Norðurlöndunum. Resecurity og SecureIT vakta netöryggi viðskiptavina sinna og láta þá vita af aðsteðjandi ógn.

Rétt fyrir áramótin hóf Resecurity samstarf við íslenska fyrirtækið SecureIT með það að markmiði að auka þjónustu sína og hækka öryggi fyrirtækja á Norðurlöndunum. SecureIT er leiðandi fyrirtæki í netöryggismálum og býður upp á ráðgjöf um netöryggi, öryggisúttektir, vottanir og ýmsar aðrar öryggis- og eftirlitsþjónustur.

Norðurlöndin hafa lengi verið leiðandi í tæknimálum og mörg helstu frumkvöðlafyrirtæki heimsins hafa komið þaðan. Má þar nefna Spotify, Skype, SoundCloud og Nokia. Norðurlöndin eru með fremstu svæðum heimsins í notkun og sköpun á tækni. Tæknilegir innviðir, tæknileg geta, hagkvæmni og aðlögun að nýrri tækni er með því besta sem gerist í heiminum.

Talsmenn Resecurity segja að samhliða vexti tækninnar og velgengni fyrirtækja á Norðurlöndunum aukist hættan á netárásum til muna og þörfin fyrir aukið öryggi að sama skapi.

„Í ljósi aukinna netógna í okkar heimshluta er nauðsynlegt að norræn fyrirtæki fjárfesti og hlúi vel að hvers kyns netöryggistækni og þjónustum sem og innri og utanaðkomandi sérfræðiaðstoð til að tryggja verðmæt gögn sem þau búa yfir. Þetta er sérstaklega mikilvægt þar sem ógnirnar á internetinu hafa aukist og netöryggi er því grunnurinn að sjálfbærum rekstri fyrirtækja. Við hjá SecureIT erum stolt af því að geta lagt lóð á vogarskálarnar með þjónustuframboði okkar og aukinni getu með samstarfinu við Resecurity sem felur í sér meðal annars uppgötvun hvers kyns netógna gagnvart stafrænum eignum fyrirtækja en líka viðbrögð ef um gagnaleka eða innbrot er að ræða. Hugmyndin er að veita mikilvægum innviðum og viðskiptavinum okkar innsýn í þessar ógnir og minnka þannig áhættu fyrirtækja og stofnana á Norðurlöndunum," segir Magnús Birgisson, framkvæmdastjóri SecureIT.

Bera sjálfkrafa kennsl á netógnir

Með því að nota gervigreind gera lausnir Resecurity fyrirtækjum kleift að bera sjálfkrafa kennsl á þær netógnir sem steðja að, meta þær og flokka út frá hættustigi. Samhliða því framkvæma sérfræðingar leit að hvers kyns ógnum gagnvart stafrænum eignum þeirra og aðstoða við greiningu og forgangsröðun viðbragða auk þess auðvitað að benda á vandamál sem annars væri erfitt að greina. Hluti af því felst í mikilvægri og umfangsmikilli vöktun á fjölmörgum ógnvöldum (e. Threat actors) víða um heim. Á sama tíma gera þær fyrirtækjunum kleift að vera skrefi á undan netglæpamönnum sem nota þróuð úrræði drifin áfram af gervigreind til að ráðast á fyrirtæki. SecureIT og Resecurity vilja auka enn frekar starfsemi sína á Norðurlöndunum og færa viðskiptavinum sínum nýjar öflugar leiðir í formi þjónustu sem finnur áhættur og ógnir til dæmis á huldunetinu (e. Dark web) og fleiri svæðum þar sem meðal annars netglæpamenn eru í samskiptum í tengslum við innbrot sem þeir standa í.

„Norðurlöndin eru miðstöð stafrænnar nýsköpunar og það sama ætti að gilda um netöryggi. Við hjá Resecurity fjárfestum mikið í rannsóknum og þróun á nýrri gervigreindartækni til að fyrirtækin hafi yfirhöndina gagnvart aukinni netógn," segir Gene Yoo forstjóri Resecurity.

„Við erum stolt af því að fara í samstarf við leiðandi fyrirtæki eins og SecureIT til að geta veitt Norðurlöndunum bestu lausnirnar á sviði netógna og áhættu (e. Cyber threat intelligence) sem völ er á."

Lausnir Resecurity til varnar netógnum bjóða upp á að senda viðvaranir til að fyrirbyggja netárásir og gera þá stafrænu ógn sem steðjar að fyrirtækinu sýnilega á yfirgripsmikinn hátt. Þessi frumlega tækni gerir stjórnendum kleift að draga úr blindum blettum og öryggisglufum með því að greina ógnina fljótt og ítarlega í gegnum meðal annars huldunetið (e. Dark web), virkni svokallaðra yrkjaneta (e. Botnets), í gegnum netgreind (e. network intelligence) og hágæða gervigreindargögn sem skilgreina ógnina. Gervigreindar-drifnar lausnir Resecurity byggja meðal annars á fimm milljörðum gagnabúta (e. Artifacts) og mörgum milljónum greininga á ógnvöldum (e. Threat actors) sem og mörg hundruð milljónum flokkaðra og greindra gagnasetta af huldunetinu (e. Dark web).

Um Resecurity

Resecurity er netöryggisfyrirtæki sem býður upp á öflugar endabúnaðarvarnir (e. Endpoint protection), áhættustjórnun og gervigreind sem aflar upplýsinga um netógnir og hvers kyns netógnagreiningu og leit. Talsmenn fyrirtækisins segja að það sé þekkt fyrir að bjóða upp á bestu gervigreindarlausnir sem völ er á. Fyrirtækið leggur áherslu á að greina mögulegar netógnir og gagnaleka snemma og vara við þeim áður en tjón verður að veruleika. Fyrirtækið var stofnað árið 2016 og hefur verið þekkt sem eitt nýstárlegasta netöryggisfyrirtæki heims. Eitt meginmarkmið fyrirtækisins er að gera öðrum stofnunum og fyrirtækjum kleift að berjast gegn netógnum óháð því hversu þróuð tæknilega fyrirtækin eru. Nýlega var það útnefnt sem eitt af tíu mest vaxandi einkareknu netöryggisfyrirtækjunum í Los Angeles af tímariti í Kaliforníu. Fyrirtækið vinnur fyrir fjölda Fortune 500 fyrirtækja, leyniþjónustur, heri, ríkisstjórnir og fleiri aðila.

Um SecureIT

SecureIT er leiðandi fyrirtæki í ráðgjöf varðandi netöryggi, úttektir, vottanir, öryggisprófanir og öryggisþjónustu (e. Managed security services). Fyrirtækið var stofnað snemma árs árið 2017 og hefur unnið með fjölda alþjóðlegra fjármálastofnana, flugfélaga, stórverslana, orkufyrirtækja, líftæknifyrirtækja og fyrirtækja á heilbrigðissviði auk stofnana í mikilvægum innviðum og með stjórnvöldum. SecureIT leggur áherslu á að veita framúrskarandi gæðaþjónustu og að aðstoða viðskiptavini við að ná og viðhalda æskilegri og nauðsynlegri öryggisstöðu. SecureIT býður upp á sérsniðna ráðgjöf, öryggisprófanir og veikleikastjórnun, áhættustjórnun, kennslu í netöryggi og endabúnaðsvarnir ásamt sólarhringsþjónustu við vöktun, eftirlit og viðbrögð (e. Managed SOC+SIEM).

> **Margir eru að endurnýta lykilorðin sín aftur og aftur og þá er yfirleitt frekar auðvelt fyrir netglæpamenn að misnota þau.**
>
> Magnús Birgisson

Framkvæma innbrotsprófanir

Magnús Birgisson, framkvæmdastjóri SecureIT, segir þjónustu fyrirtækisins geta styrkt mikilvæga innviði á Íslandi sem og á Norðurlöndunum en ýmsir netglæpir geta varðað við þjóðaröryggi.

„Við bjóðum upp á netöryggisþjónustu og höfum gert það lengi. Við erum með ráðgjöf, úttektir, vottanir gagnvart ýmiss konar stöðlum eins og til dæmis PCI-staðlinum sem er til að vernda kortaupplýsingar," útskýrir Magnús.

„Við framkvæmum ýmiss konar öryggisúttektir og framkvæmum meðal annars innbrotsprófanir á fyrirtækjum, auðvitað með leyfi frá þeim. Þá reynum við að brjótast inn í fyrirtækin og sýna hvernig hægt er að misnota hvers kyns högun, hönnun, tæknilegar varnir, öryggisstillingar og annað og með því komast yfir auðkenni, gögn og þess háttar og sýna raunverulega hvers konar tjóni netglæpamenn gætu valdið. Við höfum líka framkvæmt mikið af árásum gagnvart fólki, svo kallaðar vefveiðar, sem er ein af þeim leiðum sem er beitt til þess að komast inn í fyrirtæki. Þá er verið að plata fólk á einhvern máta til að gefa auðkennisupplýsingar eins og lykilorð og þess háttar eða aðrar viðkvæmar upplýsingar, til að geta orðið raunverulega samþykktir notendur innan tölvukerfa fyrirtækjanna. Við höfum lagt mikla áherslu á að útskýra hvað í þessu felst og hvernig fyrirtæki eigi að verjast með því að fara vel yfir málin og kenna starfsfólki góðar netöryggisvenjur og fjölga þannig öryggisvörðum hvers og eins fyrirtækis en jafnframt hjálpar það við að tryggja persónulega hagsmuni einstaklinga," segir hann.

„Þegar við höfum framkvæmt vefveiðiárás á fyrirtæki í okkar þjónustu þá förum við yfir það með þeim hversu margir féllu fyrir árásinni, hvað hefði þurft að varast og hvað hefði átt að segja fólki varðandi að um árás væri að ræða. Við segjum fólki hvernig lykilorð við komumst yfir í árásinni og kennum jafnframt fólki hvernig á að búa til lykilorð, nýtingu lykilorðageymslna svo það geti notað sterk lykilorð og margþátta auðkenningar. Margir eru að endurnýta lykilorðin sín aftur og aftur og þá er yfirleitt frekar auðvelt fyrir netglæpamenn að misnota þau eða hafa innsýn í hvernig fólk býr til lykilorð og geta þannig misnotað fólk til að framkvæma netglæpi. Eins er mikilvægt að aðskilja einkalíf og vinnu og nota ekki vinnunetfang fyrir persónulegar þjónustur en jafnframt að tileinka sér góðar öryggisvenjur úr vinnunni heima fyrir."

Magnús segir að á svokölluðu

Magnús segir að frá því í desember, þegar samstarfið við Resecurity fór af stað, hafi SecureIT látið viðskiptavini sína vita af fjölda ógna og aðstoðað þá við að bregast við þeim.

FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

hulduneti (e. Dark web) komist menn yfir ýmsar upplýsingar sem byggja fyrst og fremst á lekagögnum úr hinum ýmsu lekum. Hann segir að þar sé hægt að sjá lykilorð sem fólk hefur notað á síður eins og til dæmis LinkedIn eða Facebook, einhverja fótboltasíðu eða vefverslun eða bara hvaða síður sem er sem fólk hefur búið sér til aðgang að.

„Sérstaða okkar með samstarfsaðila okkar er meðal annars mjög aukið aðgengi að svona gögnum á hinum ýmsu stöðum, í gegnum yrkjanet þar sem búið er að yfirtaka tölvur sem felur þá líka í sér aðgengi að lykilorðum og með eftirliti gagnvart miklum fjölda ógnvalda og samskiptum þeirra við aðra.

Það eru til alls kyns varnir við netógnum, til dæmis að skipta um lykilorð reglulega og margþátta auðkenning. En þetta eru varnir sem hægt er að komast fram hjá. Til þess að byggja upp sterkt og öruggt tæknilegt umhverfi þarf að beita marglaga vörnum. Ef fyrsta vörnin dugar ekki þá þarf næsta vörn eða varnarlag að grípa eða stöðva netglæpamanninn. Við erum að reyna að hækka öryggisstig fólks og fyrirtækja og gera það meðvitað um ógnir. Við leggjum mikið upp úr kennslu. Við kennum fjölda fyrirtækja um netöryggi og hvernig fólk á að haga sér á netinu. Hvernig á að bregðast við ógnum, hvers vegna það á að vera með eldvegg á tölvunni sinni og uppfæra reglulega stýrikerfi og hugbúnað á tölvunni sinni, spjaldtölvunni eða símanum. Við kennum líka tölvudeildum fyrirtækja hvernig á að byggja upp öruggt netumhverfi og hvernig á að forrita kóða á öruggan máta og fleira í þeim dúr," útskýrir hann.

Fylgjast með milljónum ógnvalda

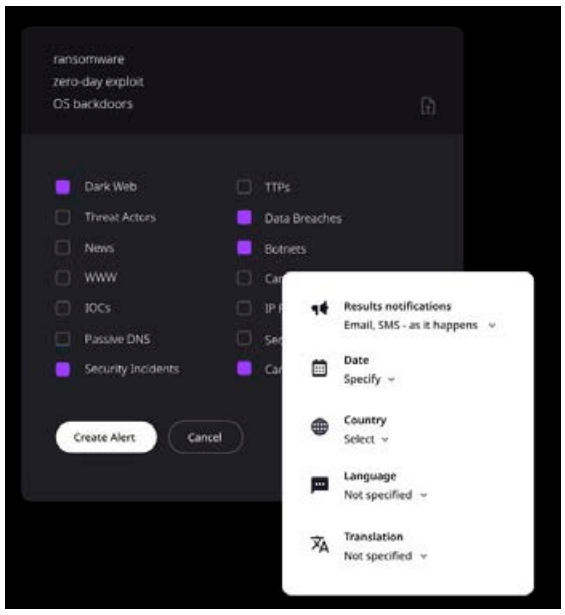
„Við erum að reyna að hækka öryggisstig fyrirtækja og stofnana sem og fólks og gera það meðvitað um fleiri tegundir netógna. Það sem kemur með samstarfinu við Resecurity er að núna fáum við gríðarlega mikið magn af upplýsingum eins og þeim sem ég hef verið að ræða um. En við fáum fleiri vinkla. Hjá Resecurity er fylgst með hátt í 30 milljónum ógnvalda um allan heim. Þeir eru á ýmsum stöðum á lokuðum svæðum á til dæmis huldunetinu að tala um netglæpi, afhafna sig og vinna saman. Oft eru þeir að biðja um hjálp við að komast lengra eða bjóða upplýsingarnar sem þeir hafa komist yfir til sölu. Þeir eru að reyna að valda tjóni," segir Magnús.

„Sumir ógnvaldar ráðast alltaf á fyrirtæki innan sama geira, sumir ráðast mikið á flugfélög, aðrir á símafyrirtæki og svo framvegis. Samstarfsaðilar okkar hjá Resecurity fylgjast með þessum ógnvöldum og við upplýsum okkar viðskiptavini um það ef búið er að komast yfir gögn frá þeim eða komast inn í einhver kerfi hjá þeim og reynum að koma í veg fyrir frekara tjón."

Frá því Resecurity og SecureIT fóru í samstarf í haust hefur fjöldi viðskiptavina SecureIT fengið upplýsingar um slík brot, að sögn Magnúsar.

„Við veitum okkar viðskiptavinum þessar upplýsingar svo þeir geti brugðist við og reynt að lágmarka tjónið, ef eitthvað varð. Það er erfitt að komast yfir svona upplýsingar. Þetta eru bara fullt af gögnum út um allt og oft erfitt að átta sig á því hvað í þeim felst. Þetta er eitthvað sem fyrirtæki berjast við alla daga, að túlka upplýsingar og meta hvort þær séu hættulegar fyrir þau. Þessir hlutir geta verið snúnir og oft hafa fyrirtæki bara mjög takmarkaðan hóp starfsmanna sem sinna þessum málum sérstaklega. Það komum við inn," segir Magnús.

Þær upplýsingar sem SecureIT hefur fundið eru meðal annars



Tilkynning um áhættu og ógn útfærð í tengslum við uppgötvun svokallaðs núlldags (e. Zero day) veikleika sem felur í sér lekagögn, yrkjanet og öryggisfrávik.

Á spjaldtölvunni sjást dæmi um fyrirtæki í vöktun, áhættur sem búið er að uppgötva og hvernig þær eru flokkaðar í öryggislausn sem kallast Risk.

lekagögn sem innihalda til dæmis kortaupplýsingar, persónugreinanleg gögn, notendanöfn og lykilorð að vefum, gagnagrunnum og hvers kyns þjónustum sem felur þá í sér að netglæpamenn geta komist yfir enn frekari viðkvæm gögn. Þetta eru dæmi um atriði sem fundist hafa með því að fylgjast með ógnvöldum og gögnum í yrkjanetum (e. Botnet) og ýmsum samskiptum og svæðum sem vöktuð eru. Magnús útskýrir að yrkjanet sé samansafn af tölvum sem búið er að yfirtaka eða ná stjórn á og þá er hægt að nota það til ýmissa vondra verka.

„Ef tölvan þín er hluti af yrkjaneti þá er hægt að nota hana í hvers kyns árásir. Til dæmis í álagsárásir (e. DDoS) sem mikið hefur verið rætt um. Þá er líka hægt að nota hana til að komast yfir gögn eins og lykilorð fólks og fleira þess háttar. Þau hjá Resecurity fylgjast með yrkjanetum í samstarfi við ýmsar leyniþjónustur meðal annars. Ef við finnum tölvu sem er hluti af yrkjaneti í gegnum þessar þjónustur, og tölvan hefur sem dæmi tengst inn á vefverslun hjá okkar viðskiptavini með ákveðnu notendanafni og lykilorði, þá er hægt að loka á að hægt sé að skrá sig inn með lykilorðinu," segir hann.

Eru með neyðarþjónustu

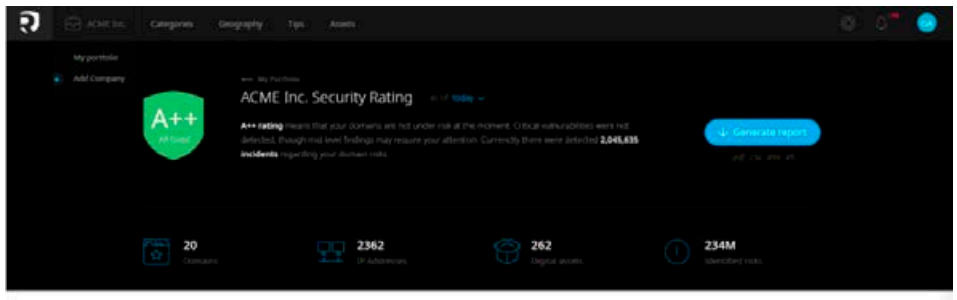
Magnús útskýrir að þegar netglæpamenn komast yfir viðkvæmar persónugreinanlegar upplýsingar hafi þeir oft hótað fyrirtækjunum að birta upplýsingarnar sem getur valdið margvíslegu tjóni, svo sem fjárhagslegu eða álitshnekki.

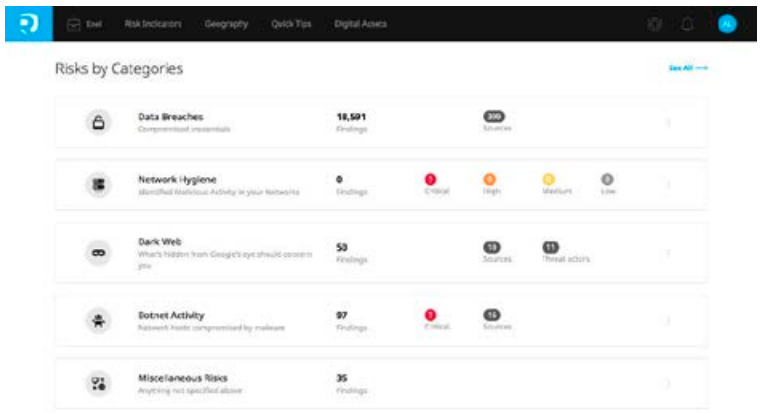
„Þetta hefur gerst og ef upplýsingarnar eru gerðar aðgengilegar munu einhverjir glæpamenn nota þær til að koma einhverjum í klandur. Það er nefnilega þannig að fólk breytir sjaldan lykilorðunum sínum inn á þjónustur eins og vefverslanir. Það breytir kannski reglulega lykilorðinu inn á tölvurnar sínar út af lykilorðareglum vinnuveitanda en það breytir ekki lykilorðinu inn á svona þjónustur nema að fá upplýsingar um að lykilorðið sé í hættu. Við höfum látið fullt af fyrirtækjum vita um slíkt til að gæta þeirra hagsmuna," segir hann.

SecureIT er einnig með neyðarþjónustu, en þá hefur fyrirtækið samið við viðskiptavini sína um að ef eitthvað komi fyrir hjálpi starfsmenn SecureIT þeim að bregðast við, annað hvort með því að koma á staðinn eða tengjast þeim í gegnum fjarbúnað. Þá er jafnframt hægt að vera með neyðarþjónustuinneign gagnvart ofangreindum netógnum.

„Við bjóðum líka upp á samninga þar sem að við aðstoðum viðskiptavinina við að semja við aðila um að fá gögnin sín aftur, til dæmis ef einhverjum tekst að brjótast inn í tölvukerfi og bjóða gögn til sölu. Það hefur gerst hér á Íslandi að gögnum hefur verið stolið eða þau gerð óaðgengileg, til dæmis í gegnum gagnagíslatöku þar sem

> **Við veitum okkar viðskiptavinum þessar upplýsingar svo þeir geti brugðist við og reynt að lágmarka tjónið.**
> Magnús Birgisson





Fyrirtækjum er gefin einkunn sem breytist út frá ógnum, ógnvöldum eða lekagögnum sem eru til staðar.

þau eru dulkóðuð og þörf er á lykli til að nálgast þau að nýju. Þá hafa verið gerðar kröfur um greiðslu hárra upphæða til að fá gögnin aftur. Þegar um er að ræða aðila sem hafa að gera með mikilvæga innviði, þá snertir þetta þjóðaröryggi," segir Magnús.

Samstarfið opnar möguleika

Magnús segir að samstarfið við Resecurity hafi hafist á síðasta ári og það hafi strax farið á flug með fjölda kynninga þar sem fyrirtækjum var sýnd öryggisstaða þeirra og aðila sem að þeim sneru, bæði þjónustuveitenda en líka birgjakeðjunnar og svo öryggi stjórnenda og hagsmunaaðila fyrirtækisins.

„Við erum að reyna að passa upp á hagsmuni okkar viðskiptavina. Ef innbrot á sér stað er ofsalega mikilvægt að hafa sérfræðinga með sér í liði sem kunna að bregðast við. Með samstarfinu við Resecurity er orðin mikil aukning á því sem við gátum gert áður. En þarna erum við með aðila sem geta gert það og hafa sinnt þessari þjónustu fyrir fjölda stórra fyrirtækja um allan heim." segir Magnús.

„Bara frá því í desember höfum við látið fjölda aðila vita um hættur sem við höfum fundið gagnvart þeim. Þar er ekki bara um íslensk fyrirtæki að ræða heldur líka alþjóðlega viðskiptavini okkar sem og samstarfsaðila okkar. Þannig að samstarfið hefur skilað heilmiklu nú þegar. Okkar markmið er að við ætlum að sjá um netógnaupplýsingar og greiningar (e. Cyber threat intelligence) á Íslandi og á Norðurlöndunum. Við vinnum nú þegar fyrir fjölda stórra fyrirtækja en við vinnum líka fyrir smærri fyrirtæki. Við bjóðum jafnframt sérstök kjör fyrir alla aðila sem tilheyra heilbrigðiskerfinu. Það er alþjóðleg stefna hjá okkur og samstarfsaðilum okkar. Samfélagið myndi ekki þola það ef viðkvæmar upplýsingar um heilsufar fólks yrðu gerðar opinberar. Við viljum að sjálfsögðu passa upp á að það gerist ekki."

Magnús segir að netógnir fari vaxandi og markmið SecureIT sé að vernda sína viðskiptavini. Öll stafræn kerfi þeirra og alla tækni sem snýr að fyrirtækinu og fólkinu sem þar vinnur.

„Viðskiptavinir hafa verið gríðarlega ánægðir með okkar þjónustu. Fólk er að standa sig vel en það er svo mikið af ógnum í gangi og erfiður leikur fyrir fólkið í fyrirtækjunum að passa upp á allt. Þess vegna erum við að veita þessa þjónustu. Hún er gríðarlega mikilvæg, ekki aðeins fyrir fyrirtækin sjálf heldur persónulega hagsmuni fólks." ■

Nánari upplýsingar um Resecurity má finna á resecurity.com. Nánari upplýsingar um SecureIT má finna á secureit.is.

Signet vörufjölskyldan auðveldar rafræna ferla hjá fyrirtækjum, svo sem undirritanir, gagnaflutning og þinglýsingar.

Helga María Jónsdóttir er vörustjóri Signet hugúnaðarlausnarinnar hjá Advania. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

Signet sparar sporin

Signet vörufjölskyldan samanstendur af vörunum Signet undirritanir, Signet transfer, Signet forms, Signet mandate, Signet innsiglanir og Signet tímastimplanir.

„Flestir þekkja Signet líklega sem undirritunarlausn en nú þegar hafa margir aðilar úr öllum geirum samfélagsins innleitt hjá sér rafrænar undirritanir með Signet. Þær eru þekktar fyrir að vera aðgengileg lausn sem hentar bæði stórum og smáum fyrirtækjum, og allar undirritanir sem framkvæmdar eru í Signet eru fullgildar, rafrænar undirritanir og jafngildar undirritun með penna," segir Helga María Jónsdóttir, vörustjóri hugbúnaðarlausnarinnar Signet hjá Advania.

„Auðvelt er fyrir einstaklinga að kaupa sér undirritanir á vefnum. Signet undirritanir gagnast líka mjög vel í dreifbýli og á landsbyggðinni, þær henta vel til undirritunar á sölu- og leigusamningum, og fyrir umboð og yfirlýsingar. Inneignin tekur sjálfkrafa gildi og hægt er að senda skjöl í undirritun um leið," segir Helga María og heldur áfram:

„Oftar en ekki byrja fyrirtæki með rafrænar undirritanir í einum tilgangi en færast svo yfir í að nota þær fyrir fleira og að lokum verða undirritanir á pappír nánast úr sögunni. Í Signet er hægt að fá mikið út úr áskriftinni þar sem ekki er greitt fyrir fjölda notenda eða teyma og því geta allir hjá fyrirtækinu haft möguleika á því að senda skjöl í undirritun, en það er fjöldi undirritana sem telur."

Rafrænar þinglýsingar

Mikil þróun hefur verið í Signet undirritunum og stöðugt verið að bæta lausnina bæði með tilliti til virkni sem og notendaviðmóts.

„Signet styður nú undirritanir fyrir rafrænar þinglýsingar þar sem innsiglaðri þinglýsingarbeiðni er komið fyrir sem viðhengi í skjalinu sem á að þinglýsa, og nú þegar eru aðilar byrjaðir að undirrita skjöl í Signet sem síðan eru send í rafræna þinglýsingu," nefnir Helga María sem dæmi um nýlega virkni.

Signet transfer er önnur Signet vara sem margir þekkja og hefur náð töluverðri útbreiðslu á Íslandi.

„Signet transfer-lausnin er öruggur, rafrænn gagnaflutningur og hugsuð sem eins konar rafrænn ábyrgðarpóstur, því í dag er tölvupóstur ekki nægilega öruggur til að senda viðkvæm gögn. Það var að áeggjan viðskiptavina sem öryggissérfræðingar Advania þróuðu Signet-lausnina. Signet sparar því sporin og lausnirnar standast ströngustu öryggiskröfur."

Dulkóðuð trúnaðargögn

Signet transfer byggir á notkun rafrænna skilríkja þannig að tryggt sé að gögnin berist réttum móttakanda.

„Gögnin eru tryggilega dulkóðuð og gengið þannig frá að aðeins móttakendur, sem sendandi skráir með kennitölu, geta sótt gögnin með rafrænum skilríkjum. Þegar viðtakandi hefur móttekið gögnin er þeim eytt sjálfkrafa úr kerfinu," skýrir Helga María.

„Signet transfer er mikilvægur liður í meðhöndlun trúnaðargagna og hefur verið notað til að senda og taka á móti trúnaðargögnum frá fyrirtækjum með allt frá einum starfsmanni til stórfyrirtækja eða stofnana. Lausnin hefur einnig verið notuð innan fyrirtækja og stofnana þar sem samstarfsfólk þarf að skiptast á trúnaðarupplýsingum eða flytja gögn milli ólíkra eininga innan fyrirtækja."

Rekjanlegar sendingar

Allar sendingar með Signet transfer eru rekjanlegar.

„Sendendur gagna geta sótt kvittun fyrir sendingu þar sem skráarheiti koma fram, ásamt því hvaða móttakendur voru skráðir og tímasetning. Þá er hægt að sýna fram á hvenær og til hvaða einstaklings eða einstaklinga gögnin voru send. Á sama hátt er hægt að sækja kvittun fyrir móttöku gagna og staðfesta að gögn sem send voru hafi verið móttekin, og hvenær," upplýsir Helga María.

Notkun Signet transfer er þegar nokkuð útbreidd og þar hafa myndast nokkurs konar samfélög sem einfaldi samskipti á milli aðila.

„Það felst mikið hagræði í að nota lausnina og sleppa við að prenta út gögn eða setja á USB-kubb sem síðan þarf að flytja með ábyrgðarpósti. Sem dæmi er Signet transfer nú þegar öflug lausn í heilbrigðisgeiranum og félagsþjónustunni, og mikið notuð af fjármálastofnunum, lögreglunni, dómstólum, lögfræðingum og fleiri aðilum sem eru að sýsla með trúnaðargögn," segir Helga María.

Tenging við innri kerfi fyrirtækja

Vefþjónustur Signet transfer gera fyrirtækjum kleift að samþætta lausnina við sín innri kerfi. Þá er hægt að láta móttekin gögn streyma beint inn í viðeigandi kerfi eða senda gögn með einum smelli úr innri kerfum fyrirtækja. Hafa helstu framleiðendur skjalastjórnunarhugbúnaðar útbúið slíkar tengingar fyrir sínar lausnir.

„Rafrænn gagnaflutningur skapar hagræðingu á svo mörgum sviðum. Fyrirtækin þurfa ekki lengur að prenta út skjöl, skanna eða geyma, og ekki þarf að sendast með pappíra, sem líka dregur úr loftmengun og fleira. Allt sparar þetta sporin og einfaldar lífið." ■

Nánari upplýsingar á advania.is

Öruggur flutningur gagna

Signet transfer er lausn til að senda og móttaka trúnaðargögn með rekjanlegum hætti.

Rekjanleiki Örugg móttaka Örugg sending Umhverfisvænt

advania