CERT-IS

Netöryggissveit

FYRIRTÆKI OG STOFNANIR

AÐ TAKAST Á VIÐ ÞJÓNUSTUROFSÁRÁSIR

ÞÝTT OG STAÐFÆRT ÚR BÆKLINGI FRÁ MSB Í SVÍÞJÓÐ

Æ algengara verður að fyrirtæki og stofnanir verði fyrir þjónusturofsárásum (Denial of Service - DOS) eða dreifðum þjónusturofsárásum (Distributed Denial of Service - DDoS) og lendi í vandræðum af þeirra völdum. Það er fremur einfalt mál að gera þannig árásir og árásarmennirnir geta verið allt frá unglingum, sem vilja sýna og sanna tæknilega færni sína án þess að íhuga afleiðingarnar, til glæpahópa með sitthvað misjafnt í huga, til dæmis fjársvik eða árás af pólitískum ástæðum. Mikilvægt er að benda á að þjónusturofsárásir eru gagnainnbrot samkvæmt 257 gr. almennra hegningarlaga og geta leitt til sekta eða fangelsisvistar. Í greininni segir:

> „Hver, sem ónýtir eða skemmir eigur annars manns eða sviptir hann þeim, skal sæta sektum …[1] eða fangelsi allt að 2 árum. [Sömu refsingu varðar að senda, breyta, bæta við, þurrka út eða eyðileggja með öðrum hætti án heimildar gögn eða forrit sem geymd eru á tölvutæku formi og ætluð eru til tölvuvinnslu.]“.

CERT-ÍS hvetur þar af leiðandi til þess að þau fyrirtæki og stofnanir, sem fyrir slíkum árásum verða, kæri þær til lögreglunnar.

Þjónusturofsárásir birtast á ýmsa vegu en snúast að jafnaði um að hindra eðlilegt aðgengi. Í stöku tilfellum getur tilgangurinn þó verið sá að leyna annarri árás sem stendur yfir. Almennt séð byggjast árásirnar á því að koma í veg fyrir að samband náist við kerfi eða samskiptanet. Til þess er beint gríðarmiklu magni gagna að upplýsingatækniþjónustu viðkomandi stofnunar. Yfirleitt verða menn varir við árás á þann hátt að aðgangur að internetinu virðist vera hægur eða stöðvast alveg, eða þá að ekki er hægt að ná sambandi við ákveðin kerfi eða vefsetur utanhúss frá eigin innra-neti eða öðrum netum.

Hægt er að gera þjónusturofsárásir á ýmsa vegu. Ein leiðin er sú að hella yfir þann sem fyrir henni verður eins mikilli gagnaumferð og mögulegt er og yfirtaka þannig alla aðgengilega bandbreidd. Það getur reynst þrautin þyngri að flokka í sundur góða og gilda umferð og þá umferð sem er hluti af árásinni. Til þess þarf sérstakan útbúnað eða jafnvel handvirka greiningu.

Þegar fyrirtæki eða stofnanir verða fyrir þjónusturofsárás, hefur það oft í för með sér bæði mikinn kostnað og álag á starfsfólkið. Hægt er að grípa til ýmissa fyrirbyggjandi aðgerða til þess að draga úr afleiðingum þjónusturofs, jafnvel þó ekki sé hægt að verjast þeim algerlega. Ef góður undirbúningur er fyrir hendi er auðveldara að takast á yfirvegaðan og skipulegan hátt á við þær aðstæður sem upp geta komið. Undirbúningurinn felst meðal annars í því að ákveða til hvaða aðgerða skuli gripið þegar eitthvað kemur upp á. Það er líka mikilvægur þáttur í undirbúningnum að skilgreina ábyrgðarsvið, hvaða starfsemi og úrræði skal leggja áherslu á og hvernig samskiptum skuli háttað, bæði innanhúss og út á við gagnvart til dæmis netveitu viðkomandi fyrirtækis eða stofnunar (Internet Service Provider - ISP).

Þeir sem eiga að koma að málum við þjónusturof verða allir að vita hvaða hlutverki þeir gegna þar og til hvers er ætlast af þeim. Til staðar verða að vera tengslaleiðir og samskiptalausnir til vara fyrir starfsemi í forgangi, vegna þess að þjónusturofsárás leiðir yfirleitt til

þess að t.d. netpóstur og vefsetur verða óvirk. Svo þarf líka að æfa neyðarviðbrögð, ekki síst vegna þess að röng viðbrögð geta jafnvel aukið tjónið og gert björgunaraðgerðir enn snúnari en annars. Mikilvægt er að hafa aðgang að atburðaskrám og afritum af umferð þegar tekist er á við þjónusturofsárásir. Séu atburðaskrár ekki fyrir hendi getur reynst erfitt að átta sig á eðli árásarinnar og gegn hvaða kerfum hún hefur beinst. Þess vegna verður að líta á gerð atburðaskráa í hinum ýmsu kerfum sem forvarnir.

Þegar unnið er að forvarnaraðgerðum, og eins þegar fyrirtæki eða stofnun tekst á við þjónusturof, er mikilvægt að gæta að því að aðgerðirnar sem gripið er til, gangi ekki gegn þeim lögum og reglum sem gilda um hina margþættu starfsemi fyrirtækja og stofnana, t.d. persónuverndarlög.

GÁTLISTI Í 4 ÞREPUM

1. AÐ FYRIRBYGGJA — HVAÐ GERUM VIÐ ÁÐUR EN ÁRÁS ER GERÐ?

Besta leiðin til þess að takmarka tjón af þjónusturofsárás er að hafa forvarnir sem bestar. Nauðsynlegt er að hafa góða þekkingu á starfsemi fyrirtækisins eða stofnunarinnar, forsendum þess og lausnum á sviði upplýsingatækni en einnig að koma á góðum tengslum út á við til þess að afla sér stuðnings og góðra ráða við þjónusturof. Þar er meðal annars átt við tengsl við viðkomandi netveitu, Netöryggissveit Póst- og fjarskiptastofnunar CERT-ÍS, lögreglu, birgja og forritara. Fyrirtækið/stofnunin þarf líka að hafa það á hreinu hvort aðgengi að tæknilegri ráðgjöf sé fyrir hendi innan eigin veggja.

Heppilegar undirbúningsaðgerðir:

- Vinnið áhættugreiningu til þess að átta ykkur á því hvaða kerfi eru mikilvægust fyrir starfsemina. Það er ekki hægt að takast á við allt samtímis og stundum þarf því að forgangsraða. Hvaða áhrif myndi þjónusturofsárás hafa, til viðbótar því að geta ekki náð sambandi við net utanhúss? Er um að ræða aðra starfsemi sem þetta gæti haft áhrif á?
- Skipuleggið og setjið í gang viðbragðsáætlun til þess að fyrirtækið eða stofnunin geti haldið áfram að starfa þó svo þjónusturof sé í gangi.
- Gerið þeim sem ábyrgð bera á starfseminni skýra grein fyrir því hvaða áhætta er til staðar hverju sinni.
- Tilnefnið hóp sem ber ábyrgð á viðbrögðum ef um þjónusturof verður að ræða í framtíðinni.
- Skipuleggið vefsetur til vara, sem hægt er að nýta sér við þjónusturof til þess að geta haldið samskiptum gangandi. Sannreynið vefsetrið reglubundið og hafið það með sem fæstum myndum og sem fyrirferðarminnstum skjölum.
- Æfið hópinn í viðbrögðum við sviðsettu þjónusturofi.
- Kannið hvaða kerfi vista atburðaskrár, til dæmis eldveggi, innbrotaskynjunarkerfi (IDS) eða syslog-netþjóna. Sé þess nokkur kostur, er gott að setja upp pakkanema til þess að taka upp umferðina sem flæðir um þann hluta netkerfisins sem árás beinist

að. Gætið þess að fyrir hendi séu atburðaskrár frá kerfum eins og eldveggjum, beinum, nafnaþjónum (DNS - Domain Name System), vefþjónum og staðgengilsþjónum.

- Hafið samband við netveituna eða þjónustuveituna til þess að kanna hvort í boði er vernd gegn árásum eða aðstoð vegna þjónusturofs.
- Kannið hvort ytri þjónustufyrirtæki geti lagt fram áætlanir um aðgerðir gegn þjónusturofsárásum. Hafið viðbrögð gegn þjónusturofsárásum með í samningum um þjónustu upplýsingatæknifyrirtækja.
- Kannið þörfina fyrir annars vegar varavefsetur hjá annarri netveitu og hins vegar tengingar við fleiri en einn netþjónustuaðila.
- Skilgreinið grunnlínu fyrir eðlilegt álag á tölvukerfið og komið á fót góðu eftirliti með henni til þess að uppgötva árás sem allra fyrst.
- Beitið álagsdreifingu til þess að dreifa umferðinni og álaginu á marga bakliggjandi netþjóna. Sumir álagsdreifar eru jafnframt búnir vernd gegn dreifðum þjónusturofsárásum (DDoS).
- Dreifið myndum og skjölum á marga netþjóna, til dæmis á aðra nethluta.
- Notið ykkur samræmt snið atvikaskráa til þess að fá sem greinilegasta yfirsýn frá fleiri heimildum.

2. AÐ BERA KENNSL Á VANDANN —HVAÐ GERÐIST?

Það er fyrir öllu að fá sem fyrst yfirsýn yfir þjónusturofsárás sem gerð er til þess að geta gripið til réttra og viðeigandi ráðstafana.

Viðeigandi ráðstafanir:

- Í fyrsta lagi þarf að gera sér grein fyrir árásinni og, sé þess nokkur kostur, að greina atvikaskrár til þess að átta sig á því hvers eðlis árásin er og gegn hverju hún beinist. Mikilvægt er að vista allar gerðir atvikaskráa sem hægt er að nýta sér við greiningu á atburðinum.
- Skjalfestið allt sem skiptir máli. Hver gerði hvað, við hverja var haft samband, til hvaða ráðstafana var gripið og á hvaða tíma var þetta gert? Þá verður auðveldara að gera skýrslu um málið síðar. Hafi fyrirtæki eða stofnun yfir að ráða nægilega öflugri rannsókna- og tæknideild, er hægt að byrja að greina það sem gerðist. Oft er þó betra að leita aðstoðar sérfræðinga utan frá. Nauðsynlegt er að koma í veg fyrir að sönnunargögnum sé spillt.
- Bendi niðurstöður til þess að eitthvað óvenjulegt standi yfir, ætti að taka ákvörðun um aðgerðir til að draga úr áhrifum þess og halda áfram að greina atvik.
- Þegar staðfest hefur verið að um þjónusturofsárás sé að ræða, skal reyna að stöðva hana eða takmarka afleiðingarnar sem allra mest.

- Hafið samband við netveitu fyrirtækisins/ stofnunarinnar með beiðni um að loka fyrir þær IP-tölur sem að árásinni standa. Gætið þess að hafa alla tengslalista uppfærða og kanna reglulega hvort upplýsingar á þeim séu réttar.

Mikilvægt er að safna saman eftirfarandi gögnum til frekari greiningar:

- Atvikaskrám frá netveitum, eldveggjum, beinum, innbrotaskynjunar- og varnarkerfum, netþjónum, póstþjónum, lénaskráningarkerfum, netgreiningarkerfum o.s.frv.
- Gögnum frá þeirri tölvu eða tölvum sem þjónusturofsárásinni er beint gegn.
- Upplýsingum um hvers eðlis árásin var.

Eftirfarandi forrit er til dæmis hægt að nota til þess að greina atvikaskrár í tölvunetinu:

- Wireshark (greinir Pcap-gögn).
- Argus (greinir NetFlow- og Pcap-gögn).
- Nfdump (greinir NetFlow-gögn).

3. AÐ TAKMARKA - HVAÐ? HVERNIG? HVENÆR? HVAR? HVER?

Um leið og náðst hefur yfirsýn yfir það sem gerðist verður að snúa sér að því að lágmarka skaðann af þjónusturofinu. Best er að einangra viðkomandi stað, sé þess nokkur kostur. Sé um alvarlega árás að ræða er mikilvægasti tengiliðurinn netveita fyrirtækisins/ stofnunarinnar. Hún er fyrsta tengingin við internetið og þar er hægt að grípa til ákveðinna varnar- og mótvægisaðgerða.

Ekki er algengt að fyrirtæki/ stofnun geti sjálf brugðist við og leyst úr þjónusturofi upp á eigin spýtur. Oft þarf að leita til annarra fyrirtækja til þess að stöðva eða draga úr árás, til dæmis til netveitna, netþjónustufyrirtækja, Netöryggissveitar Póst- og fjarskiptastofnunar og lögreglu. Spyrja þarf sem fyrst ákveðinna spurninga þegar atvik verða:

- Hefur fengist staðfest að um þjónusturofsárás sé að ræða?
- Eru til atvikaskrár af tölvunetinu eða viðkomandi kerfi?
- Um hvers konar árás var að ræða?
- Er hægt að hindra umferð í einhverjum netbúnaði?
- Hvað hefur fyrirtækið/stofnunin gert til þess að takmarka/stöðva árásina?
- Hefur verið haft samband við netveitu eða netþjónustufyrirtæki?
- Hefur verið haft samband við Netöryggissveit Póst- og fjarskiptastofnunar?
- Sér utanaðkomandi aðili um rekstur á kerfinu?

Nauðsynlegt er að setja upp pakkanema sem allra fyrst og taka afrit af umferðinni til þess að átta sig á því hvernig árás var gerð á fyrirtækið/ stofnunina og fá góða heildarmynd af stöðunni. Það er auðvitað líka lykilatriði að taka með í reikninginn alls

konar atvikaskrár af tölvunetinu og úr öðrum kerfum til þess að fá heildarmynd af atvikinu.

Til þess að takmarka eða stöðva árás:

Hafið samband við netveitu eða netþjónustufyrirtæki. Þar eru í boði lausnir af ýmsu tagi til varnar þjónusturofsárásum.

Grunnstillið síur (ACL - aðgangsstýringarlista) í tölvunetbúnaði. Stundum er hægt að útbúa síu á grundvelli greiningar sem gerð var á meðan verið var að bera kennsl á vandann.

4. AÐ KOMA MÁLUM Í SAMT LAG Á NÝ OG LÆRA AF REYNSLUNNI

Beita skal hefðbundnum aðferðum til þess að koma þeim tölvubúnaði og –kerfum í upprunalegt horf, sem orðið hafa fyrir árás. Endurheimt kerfi þarf að rannsaka og öryggisprófa áður en þau eru tekin í notkun á ný.

Einnig þarf að notfæra sér reynsluna af atvikinu til þess að hindra árásir í framtíðinni og lágmarka tjón af þeirra völdum. Atvikaskýrsla gegnir því hlutverki að taka saman kerfisbundnar upplýsingar um reynsluna af atvikinu.

Sé um umfangsmikla þjónusturofsárás að ræða, er oft mjög gagnlegt að safna sjónarmiðum og reynslu þeirra sem þátt tóku í starfinu gegn árásinni, draga þær saman og kynna svo skýrsluna á eftirfylgnifundi þar sem allir fundarmenn hafa tækifæri til þess að ræða hana. Sé um minniháttar atvik að ræða með litlum hópi fundarmanna, er hægt að taka sjónarmið og reynslu saman á fundinum sjálfum.

Mikilvægt er að benda ekki á neinn sérstakan blóraböggul. Gætið þess að gera fundarmönnum grein fyrir því. Markmiðið með eftirfylgnifundinum er að efla getu fyrirtækisins/ stofnunarinnar til þess að takast á við önnur atvik síðar.

AÐ LÁTA VITA AF ÞVÍ SEM GERÐIST

Það kemur sér vel í viðbrögðum og endurheimt að hafa skjalfest vinnulag og afla sér þjálfunar, en það þarf líka að hafa samband við ytri aðila svo sem blaðamenn, íbúa og/eða aðra hagsmunaaðila. Ef árás gerir það að verkum að sum eða jafnvel öll þjónusta fyrirtækis/ stofnunar verður óaðgengileg, er mikilvægt að koma þeim upplýsingum á framfæri. Lykilatriðin eru tvö: Hefur verið gerð samskiptaáætlun? Veit fólk hvað það ætlar að segja?

Eftirfarandi upplýsingar þarf meðal annars að gefa:

- Hvað gerðist og hvaða afleiðingar það hafði.
- Hvað reikna má með að langan tíma taki að kippa málum í liðinn.
- Hvenær búast má við nánari upplýsingum og hvar þær verður að finna.

Innri samskipti skipta einnig miklu máli. Þau sem svara í síma verða að vita hvaða upplýsingar þarf að gefa þegar fólk byrjar að hringja inn og kvarta.

AÐ LÆRA AF REYNSLUNNI

Það ber að huga að því að þjónusturofsárásir eru algengar í netheimum og eitt það fremsta vandamál sem menn kljást við að sökum þess hversu tiltölulega einfalt það er að viðhalda slíkum árásum. Þá gildir að læra af reynslunni í hverju því formi sem hún

kemur mönnum fyrir, hvort sem það gildir að bæta úrræði sem ekki virkuðu eða stofna til nýrra varna og aðgerða sem hafa reynst mönnum vel. Þó vandamálið herji marga er þó einnig til staðar hjálp, bæði í formi þjónustuaðila sem bjóða upp á úrræði og ráðgjöf, sem og upplýsingar um bestu venjur fyrir tæknilega inniviði fyrirtækisins.