Mis juhtub, kui meid tabab magnetimpulss, küberrünnak või suur kaablirike?

30. aprill 2018 - 0:29 Autor: Kaido Einama

Kunagine Linxtelecom, praegune CITIC CPC ühendab meid välismaailmaga ja pakub ka serverikeskusi paljudes erinevates regioonides. Andmekeskused ja ühendused nende vahel on infoühiskonna närvivõrk. Uurisime CITIC CPC Euroopa juhi James Halberstadti käest, mis juhtub, kui midagi suurt juhtub (näiteks elektromagnetiline impulss ehk EMP, kaablirike või muu suur andmehäving) ja kuidas inimkond sellest supist välja tuleb.

Mis juhtub kõikide nende andmetega, mis on talletatud serveritesse üle maailma EMP (elektromagnetilise impulsi) korral, näiteks päikesest? Kas CITIC CPC on selliste katastroofide eest kaitstud? Kuidas te kaitsete oma andmekeskuseid võimalike välismõjude eest?

Iga võimalikku ohtu meie süsteemidele ja andmetele tuleb võtta tõsiselt ning tegelikult ei räägita sel teemal avalikkuses piisavalt. Rahvas peab teadma, et kriitilise tähtsusega riiklik infrastruktuur toetub mitmetele süsteemidele, milleta oleks juhtival administratsioonil väga kiiresti väga keeruline tegutseda. Sellise juhtumi jaoks valmistudes tuleb kaaluda sellega kaasnevaid riske ning selle juhtumise tõenäosust ning ehkki EMP rünnak on väga ebatõenäoline, oleksid selle tagajärjed äärmiselt laastavad.

Eelnevalt mainitud üldised süsteemide kaitsmise põhimõtted kehtivad ka siin: andmete geograafiline eraldatus ning teenusepakkujate mitmekesisus on parim kaitse. EMP rünnaku korraldamine on erakordselt keeruline ning kui mõnel terrorirühmitusel õnnestuks seda korraldada, oleks see tõenäoliselt linna piires lokaliseeritud. Järelikult aitaks süsteemide geograafiline eraldamine andmeid kaitsta. Tasub ka meeles pidada, et olenemata sellest, mis seisundis kellegi süsteemid on, on siiski tõenäoline, et lõppkasutajaid tabab selline sündmus väga rängalt, näiteks oleksid kõik nende sülearvutid ja nutitelefonid täielikult välja lülitatud. Seega on kellegi süsteemide seisund ainult üks element kogu võrrandis.

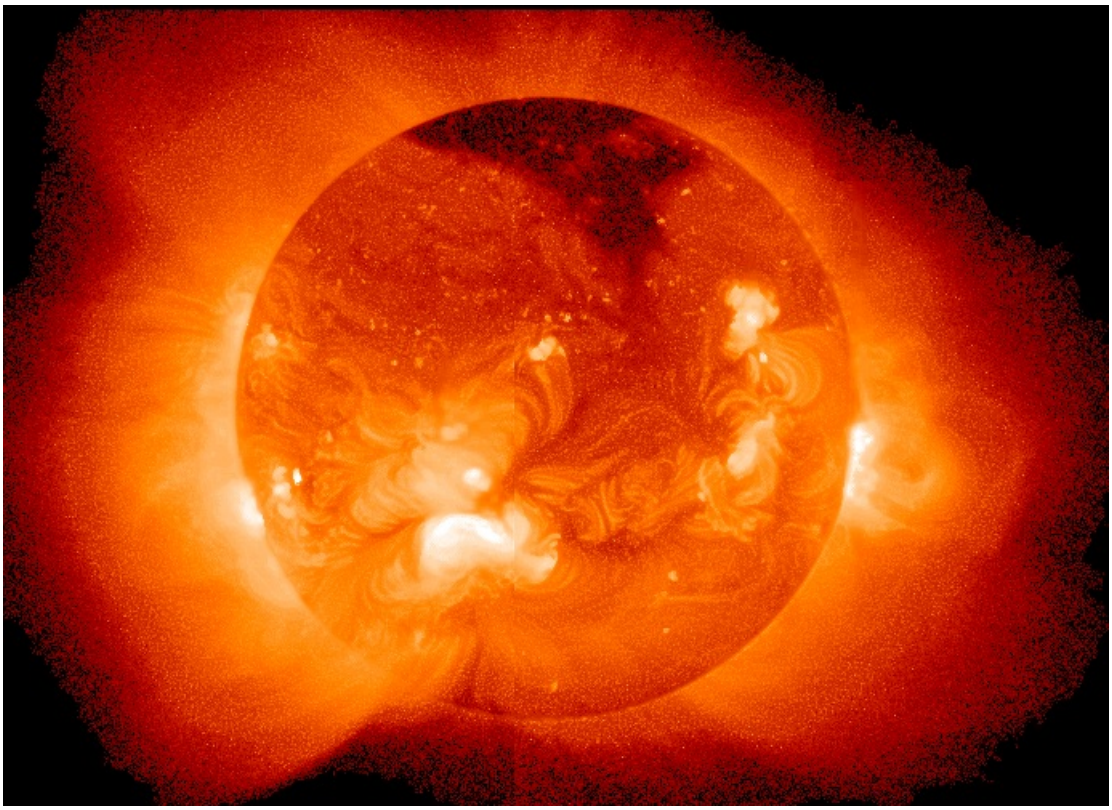

Foto: NASA

Aeg-ajalt juhtub seda, et veealused kaablid tõrguvad ja lähevad katki. Kuidas ja milliste kaablitega on Eesti ülejäänud maailmaga ühendatud? Mis tagab selle, et see ühendus ei katkeks kunagi?

Tõepoolest esineb mõnikord selliseid *force majeure* olukordi ning kõik viimased sündmused, mis on Eestit mõjutanud, on tulenenud laevade ankrutest.

Eesti on muu maailmaga ühendatud mitmete kaablisüsteemidega, mis lähevad põhja suunas Helsingisse ning lääne suunas üle Läänemere, maandudes eri kohtades Rootsis. Lisaks on Eestil olemas maismaa ühendused, mis lähevad lõuna suunal teistesse Balti riikidesse. CITIC Telecom CPC omanduses olevad Balti mere allveekaablisüsteemid koosnevad erinevatest lõunasuunalistest süsteemidest suunal Stockholm <-> Tallinn <-> Helsinki ja põhjasuunalistest trajektooril Helsingi-Stockholm. See ringikujuline disain kaitseb katkestuste eest, kuna andmeliiklust on katkestuse ajal võimalik suunata ringi teisele poolele.

Merekaablite parandamine ei ole lihtne töö, kuna see sõltub ilmastiku tingimustest ning vajab spetsiaalseid laevu ja varustust, mis peavad enamasti väga suuri distantse läbima, et leida kaablis olev katkine koht üles. Seetõttu on võimekus andmeliiklust ümber suunata ainus kindel viis kaitsta end katkestuste eest.

CITIC Telecom CPC võrgus on lisaks Läänemere kaablisüsteemile ka kolm füüsilist kaablit, mis ühendavad Eestit ülejäänud maailmaga. Olles oma optilise kaabliga ühendatud Narva või Tartuga, võimaldab see meil kasutada maismaa kaablisüsteeme, mis ühendavad Eesti läbi teiste Balti riikide muu maailmaga. Nii on tagatud lisaturvalisus ka sellistes väga ebatõenäolistes olukordades, kui kõiki merealuseid kaableid peaks tabama samaaegne rike.

Kuidas te kaitsete oma allveekaableid sõjamängude eest, mida meie regioonis on üha rohkem toimumas?

CITIC Telecom CPC Läänemere kaablid on disainitud vastavalt rahvusvahelistele standarditele, mis kehtivad veealustele kaablisüsteemidele, mis tagab, et nad on tugevdatud ning kaitstud juhuslike üleskaevamiste ja lõigete eest. Lisaks on kaablite koordinaadid ning maandumisjaamade asukohad registreeritud vastavate valitsusautoriteetide juures, mis garanteerib, et meie vara on samamoodi kaitstud ja järelvalve all nagu igasugune muu riiklik vara või kriitilise tähtsusega riiklik infrastruktuur.

Ent kuna me ei ole meresõjanduse eksperdid, siis meil pole võimalik garanteerida, et meie kaablid suudaksid vastu pidada mereväe- või muudele võimalikele välisriikide poolt algatatud rünnakutele. Marsruutide mitmekesisus nii vee all kui maa peal on jätkuvalt parim võimalik kaitse ühe rünnakuvektori vastu.

Mitmed ettevõtted arvavad, et pilves talletatavad andmed on sisuliselt avalikud andmed,

kuna keegi ei tea tegelikult, kellel on nendele andmetele ligipääs olemas ja kuidas. Kas see on ka päriselt nii? Kuidas te neid ettevõtjate hirme vähendaksite või ümber lükkaksite?

Mitmed valitsused maailmas võtavad aina rohkem omaks nn nõudluspõhist või teenuspõhist pilvetöötlusmudelit. Eesti on selles valdkonnas juhtival positsioonil, olles mitmed teenused oma inimestele teinud kättesaadavaks e-teenustena, näiteks e-valimised, mis on olemas juba aastast 2007, digiretseptid ning isegi e-residentsus. Selliste teenuste eelised hinna ning reageerimiskiiruse osas on ilmselged, kuna sellega kaasnevad väiksemad riistvara kulud ning võimekus teenuseid suuremaks või väiksemaks skaleerida peaaegu koheselt, näiteks valimisperioodil või gripiepideemia ajal.

See aeg, mil ettevõtete ja riigiasutuste IT-juhtidel oli vaja oma silmaga näha ja käega katsuda servereid ning võrguseadmeid asutuse isiklikus andmekeskuses, on juba peaaegu minevik. Kuigi see võib kõlada ebaloogiliselt, siis korrektse kasutuselevõtu korral võimaldab see tohutult parendada andmete ja süsteemide üleüldise turvalisuse kvaliteeti ja tugevust.

Samuti tuleb meeles pidada, et pilvede kasutusele võtmiseks on mitmeid meetodeid, alates IaaS-ist (infrastruktuur teenusena) kuni SaaS-ini (tarkvara teenusena). IaaS teenused pakuvad virtuaalmasinate kujul infrastruktuuri loomiseks vajalikku riistvara ning baasoperatsioonisüsteeme. Sealjuures jääb ettevõttele täielik kontroll oma kasutajate andmebaasi üle nii, et IaaS teenuse pakkujal sellele mingisugust ligipääsu ei ole. Ettevõtte saab vabalt paigaldada, seadistada ning hallata samasid turva-, varundus- ning avariitaaste kaitseteenuseid, mida nad saaksid kasutada, kui nende süsteemid paikneksid nende isiklikus andmekeskuses, ning samas võib ettevõtte rahus tegutseda, kuna IaaS teenuse pakkuja andmekeskuse füüsiline turvalisus ning spetsifikatsioonid on palju tugevamad, võrreldes sellega, mida pakuks nende teenuste majutamine kasutajate asukohas.

Kui ettevõtted soovivad paigaldada SaaS teenust, mis juhul kasutab ettevõte teenusepakkuja tarkvara kasutajate ja litsentside arvu kohta ning laadib seeläbi üles tundlikke lõppkasutajate andmeid, siis rakendub teenusepakkujatele uus andmekaitse üldmäärus ehk GDPR, mis asendab varasemat Euroopa Parlamendi ja nõukogu direktiivi 95/45/EÜ ning mis hakkab kehtima 25. mail 2018. See määrus kehtestab täpselt, mis kohustused on andmete omanikel ning töötlejatel, ning sellega kaasnevad suured trahvid mitteallumise korral, milleks on kuni 4% ettevõtte ülemaailmsest käibest või 20 miljonit eurot, kumb iganes on suurem summa. Määrus hakkab kehtima kõikidele ettevõtetele, kes tegutsevad Euroopas, kaasa arvatud suurettevõtetele nagu Facebook.

Eesti avas Luksemburgis maailma esimese andmesaatkonna. Kas teie arvates on see turvaline, kui üks riik hoiab oma andmeid väljaspool oma riiki? Kui jah, siis mis garanteerib sel juhul kõrge turvalisuse? Kui ei, siis miks?

Kõik ettevõtted ja riigiasutused peavad tagama, et neil oleks tugev turvalisus ning avariitaasteplaan, et nad saaksid kaitsta oma võtmesüsteeme ja andmeid. See võib olla vajalik selleks, et kaitsta end süsteemitõrgete korral, ent üha enam on see oluline ka selleks, et kaitsta end küberrünnakute eest, mis võivad ühe ettevõtte täiesti halvata, kui nad kaotavad andmeid, kui neilt varastatakse tundlikke intellektuaalomandeid või kui seeläbi lekitatakse andmeid, mis tekitavad kahju ettevõttele või indiviididele. Andmete kaitsmine selliste olukordade ennetamiseks ja neist taastumiseks on kõige olulisem ning seetõttu on isegi soovituslik rakendada geograafilist eraldatust ning teenusepakkujate mitmekesisust.

Kõigil suurtel valitsustel maailmas on võimekus nende piire ületavaid andmeid vahelt kinni püüda. Vanasti oli võimalik telefoniliine pealt kuulata. Tänapäeval aga on olemas palju peenemad meetodid, millega tegutseda üha keerulisemas interneti- ja andmeülekannete maailmas. Riigiti erineb vaid see, mis taseme autoriteeti ning volitust on vaja kohalikult kohtult, et õiguskaitseasutused saaksid loa otseselt andmetele ligi pääseda või kohustada asjakohast teenuspakkujat seda ligipääsu neile pakkuma.

Küsimus, kas tundlikke valitsusandmeid saab ja peaks hoiustama riigist väljaspool või piisaks riigi sees andmete eraldamisest, sõltub mitmest asjaolust:

1. Hea tava soovitab kriitiliste süsteemide jaoks geograafilist eraldatust ning teenusepakkujate mitmekesisust. Ent missugust täiendavat kaitset loodad sa saada andmete väljaspool riiki hoiustamise eest?
2. Kui sa viid oma andmed riigist välja, siis pead arvestama ka kohaliku jurisdiktsiooni seaduste ja määrustega. Kui see riik asub Euroopa Liidus, kehtivad sellele ELi seadused. Kui sa viid oma andmed aga kaugemale, näiteks Venemaale, Ameerikasse, Hiinasse või Austraaliasse, siis pead sa leppima asjaoluga, et nendel valitsustel on teatud olukordades õigus nõuda ligipääsu sinu andmetele ning sa pead end selles olukorras tundma mugavalt ja samas tagama, et see ei ohusta sinu kohalikke seaduseid või veel enam, sinu riiklikku julgeolekut kodus.

Eesti on ainulaadsel positsioonil tulenevalt oma ajaloolisest eraldumisest Nõukogude Liidust 1991. aastal ning 2007. aasta küberrünnakust, mis väidetavalt pärines Venemaalt ning mis lülitas 50 veebiteenust samaaegselt välja. Krimmi annekteerimine Venemaa poolt 2014. aastal tõstis selle teema

taas päevakorda, tekitades avalikku arutelu. Seetõttu üritab Eesti mõõta, kas parem on hoida kõiki oma andmeid oma piiride sees, misläbi nad on haavatavamad üheainsa rünnaku korral, või on turvalisem nad viia teise jurisdiktsiooni, kus Eesti kontroll ja omandiõigus nende andmete suhtes on vähendatud.

Mis on teie plaanid CITIC Telecom CPC Euroopa juhina meie regiooni ning täpsemalt Eesti jaoks?

Eesti on atraktiivne turg, kuna ta on juhtinud teed veebiteenuste reklaamimise vallas, mistõttu on Tallinnasse tekkinud väga palju tehnikavaldkonna idufirmasid. Investeerimise seisukohalt jäetakse Balti riigid tihtipeale kõrvale ning eelistatakse Põhjamaid, ent CITIC Telecom CPC, millel on kohalolek TLL-IX-is (Tallinn Internet Exchange sõlmpunkt), opereerib Metro ühendust Tallinnas, mis on ühendatud globaalse võrgustiku infrastruktuuriga, millel on tugev katvus kogu Baltikumis, Ida-Euroopas, Venemaal ja Sõltumatute Riikide Ühenduses ning madala latentsiga ühendus Aasia ning Hiinaga. Võrguteenuste pakkuja Baltikumis, kes suudab vastata nii kohalikele kui ka globaalsetele nõuetele, on ainulaadne. Meie pakkumiste portfell ei ole aga piiratud ainult era- (Ethernet, MPLS) ja avalike (interneti otseühendus) võrkude ühenduvusega. Seda täiendavad 15 globaalset pilvekeskuse sõlme, mis pakuvad meie ettevõtetest klientidele Iaas ning turbetarnija teenuseid. Meie Euroopa ning Hongkongi ja Hiina äride ühenduste tugevdamine võimaldab meil kasu saada ka Uue Siiditee (One Belt, One Road) investeeringutest, mis omakorda võimaldab Eesti ettevõtetel julgelt kasutusele võtta nii kohalikku kui ka globaalset ühenduvust ning pilveteenuseid.

Tegijad
Uudised
Andmeside
Serverid
Võrguseadmed