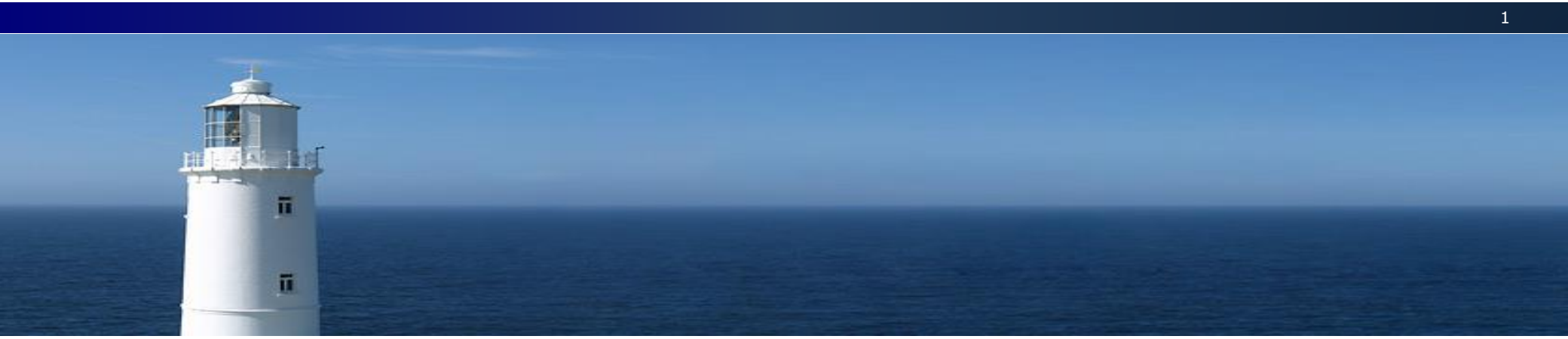


Tulevatko kyberturvallisuusuhat ulkoa vai sisältä? -- Näkemys nykyajan uhkakuviin

Harri Kreus, johdon konsultti

Inhimillinen tekijä turvallisuuden näkökulmasta

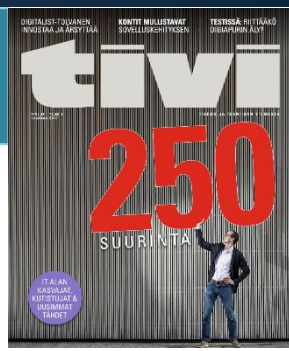
27.5.2021

Pari sanaa meistä yhtiönä ja puhujasta

Tuomme lisäarvoa ja kilpailuetua asiakkaillemme korkean tason konsultointi- ja asiantuntijapalveluilla ja näiden avulla tuotettavilla ratkaisuilla.

Yhtiömme

- Henkilöstönsä omistama palveluyhtiö
- 55 työntekijää - keskimäärin yli 20 vuoden kokemus alalta
- Aktiivisia asiakkaita tällä hetkellä 16 – kaikki alansa merkittäviä toimijoita
- Finanssi, teollisuus ja julkishallinto: kyber- ja tietoturva aina osana hankkeitamme



TE arvosana 10,0.

Liikevaihto 2019

10,6 meur.

Harri ”Hakki” Kreus

- Yli 30 vuoden kokemus ICT alalta liiketoimintakriittisten järjestelmien parissa; Novo Group, WM-Data, SYSOPENDIGIA, AuroraNet, AuroraDS, Profit Consulting
- Ex-meriupseeri viimeisenä positiona Suomenlahden Meripuolustusalueen tietohallintopäällikkö eli kylmänsodan veteraani
- Tehnyt hankejohtamista, jossa tieto-/kyberturvallisuus osana
  - Finanssi, telecom, teollisuus ja julkishallintotoimialoilla
  - BS7789, ISO27001, PCI DSS, KATAKRI, ISO 9001:2000, AQAP 2110
  - Zachman, TOGAF, DoDAF, FEA, NATOAF. PVTAK

Kyber-, hybridi-, verkkokeskeinen jne.

Niin kauan kuin on ollut tietoa, sitä on pyritty hankkimaan omaksi eduksi vilpillisin ja rikollisin menetelmin ja vastaavasti suojaamaan omaa tietoa

Ilmiönä ikivanha, joskin teknologia tuonut uusia ulottuvuuksia ja mahdollisuuksia

- Sun Tzu : ”Jymäyttämisen taito”
  - Harhauttaminen, väärän informaation syöttäminen vastapuolen päätöksentekoon
  - Lineaarinen vs. epälineaarinen vaikuttaminen
- Gaius Julius Caesar: ”Rakastan petoksia, mutta vihaan pettureita!”
  - Tiedon suojaaminen salakirjoituksella
- Sir Francis Walsingham; Britannian tiedustelupalvelutoiminnan perustaja
  - Mary Stuartin viestinnän ja salakirjoituksen murtaminen (Babingtonin koodi)
  - Espanjan Suuren Armadan valmistelut ja liikkeet; Lordi Seymour: *”You have fought more with your pen than many have in our English navy fought with their enemies"*

Kyber-, hybridi-, verkkokeskeinen jne.

Niin kauan kuin on ollut tietoa, sitä on pyritty hankkimaan omaksi eduksi vilpillisin ja rikollisin menetelmin ja vastaavasti suojaamaan omaa tietoa

- Mikä sitten *on* muuttunut?
  - Modernin tiedonvälityksen ja sosiaalisen median myötä kyky vaikuttaa nopeasti suuriin ihmisjoukkoihin
  - Tiedosta on tullut yhä enemmän pääomaa ja haluttua kauppatavaraa
  - Kyberoperaatiot mahdollistavat painostamisen/vaikuttamisen 24/7 ja esim. sääoloista riippumatta
  - Kineettinen vaikuttaminen eli fyysisen voiman käyttö ja siihen valmistautuminen ei kuitenkaan ole poistumassa keinovalikoimasta
  - Ei-kineettinen asevaikutus:
    - Pankki-, energia-, liikennejärjestelmien häirintä tai lamauttaminen
    - Gerasimovin doktriini 2013: ”Lineaarinen, kineettinen vaikuttaminen viimesijainen keino”
  - Kyberin nouseminen uhkakuviin on saattanut luoda illuusion, että tulevaisuudessa sodat ja konfliktit tapahtuvat vain kyberulottuvuudessa.
  - Digitaalisessa yhteiskunnassa onnistunut kyberoperaatio voi aiheuttaa mittavat vahingot, eikä ihmishenkien menettämiseltäkään voida välttyä

Operaatiomuodot ja operoijat

Niin kauan kuin on ollut tietoa, sitä on pyritty hankkimaan omaksi eduksi vilpillisin ja rikollisin menetelmin ja vastaavasti suojaamaan omaa tietoa

- Operaatiomuodot
  - Tiedustelu-vastatiedustelu
    - Tiedustelussa olennaista on olla paljastumatta
  - Harhauttaminen
    - Harhatiedon syöttäminen (paljastumatta)
    - PsyOp: esim. halutaan paljastua helposti/tahallaan, jolloin vastapuoli ihmettelee operaation kömpelyyttä/tarkoitusperiä => psykologinen vaikutus
  - Offensiivinen (hyökkäyksellinen)
    - Ei-kineettinen vaikuttaminen
    - Hyökkääjään salaaminen mahdollisimman pitkään luoden hämmennystä/epävarmuutta tehostaen vaikutusta
  - Defensiivinen (puolustuksellinen)
    - Oman toiminnan ja tiedon turvaaminen, vastaharhautus, ”hiirenloukut”

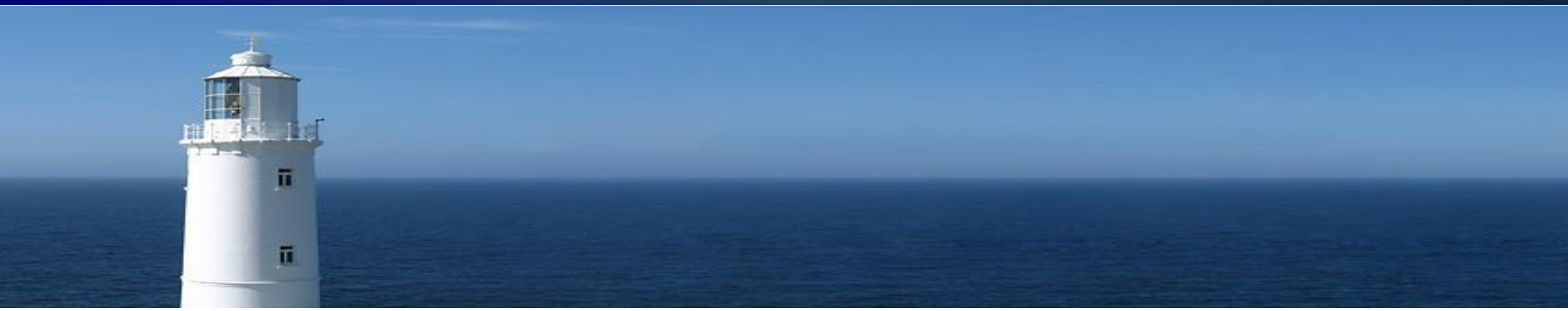
Operaatiomuodot ja operoijat

Niin kauan kuin on ollut tietoa, sitä on pyritty hankkimaan omaksi eduksi vilpillisin ja rikollisin menetelmin ja vastaavasti suojaamaan omaa tietoa

- Operoijat
  - Yksityiset hakkerit/ryhmittymät
    - Tiedon paljastukset, kiristys
    - Esim. WikiLeaks
  - Ammattimaiset ryhmittymät (kyberin Wagnerit/Blackwaterit)
    - Usein suora yhteys valtiollisiin toimijoihin alihankkijoina ”plausible deniability”
    - Järjestäytynyt kyberrikollisuus
    - Tiedustelu/häirintä/harhauttaminen
  - Valtiolliset toimijat
    - Tiedustelu/harhauttaminen/offensiivinen toiminta

Inhimillinen tekijä

- Elokuvat luovat vaikutelmaa, että hakkereilla/hyökkääjillä on käytössään ylivertainen teknologia, jolle ei vain voi mitään
- Kyber- ja tietoturvapoikkeamissa kuitenkin inhimillisen tekijän vaikutus on todella suuri
- Kevin Mitnickin saavutukset perustuivat pitkälti ”sosiaaliseen hakkerointiin” eli inhimillisen tekijän hyväksikäyttöön
- Järjestelmien oletusasetukset, heikot salasanat, päivitysten laiminlyönti, ”luotettavan kumppanin hyväksikäyttö”, naiivius ja sinisilmäisyys jne…
- Mutta: myös tahallinen myötävaikutus
  - Miksi joku suostuu avustamaan?
  - MICE
    - Money
    - Ideology
    - Consciousness
    - Ego
  - Kiristys yms. perinteiset värväyksen keinot…



Case-esimerkkejä

Huom! Vaikka joistain tapauksista on jo aikaa, se ei tarkoita etteivätkö kokemukset/opit pätisi edelleen

Luotettavan toimijan kautta soluttautuminen

- Milleniumin yhteydessä suuri suomalainen operaattori päätti ALL-IP murrosta odottaessaan päivittää milleniumin vuoksi IN-keskuksensa(IN = Integrated Network) yhden laitetoimittajan laitteille
- Merkittäviä muutoksia älykeskusten väliseen SS7-NMS -yhteiskanavamerkinantoon => jos pääset perille YKM-signaloinnista =>yippee-kay-yeey
- Venäläinen kumppani operaattorin kansainvälisen liiketoiminnan yksikön kautta ”YKM:ssä välillämme häikkää, haluaisimme asentaa snifferin monitorointia varten…”
- Muutamaa viikkoa myöhemmin laitetoimittaja: ”Sopiiko, että amerikkalainen asiakkaamme AT&T…

  => AT&T:n ja USA:n tiedusteluviranomaisten läheinen yhteistyö on kylmänsodan parhaiten tunnettuja julkisia salaisuuksia
- Operaattorin turvallisuusjohtaja tämän jälkeen: ”Jahas, tehdäänkös sitten kalenterivaraukset myös Mossadille, GCHQ:lle, DGSE:lle ja BND:lle?!?

Sosiaalinen hakkerointi ”lirkuttelemalla”

- Netcentric Warfare aikakaudelta 90-luvun alkupuolella
  - (Siis ajalta, jolloin me kylmänsodan veteraanit olimme nuoria ja komeita, nyt enää ”ja” ☺)
- Tekeytymällä harjoitukseen osallistumattoman aluksen viestiupseeriksi ja pyytämällä salaamattomaan faksiin viestiliikenneperusteet (salausavaimet) ja ne saatiin
- Tämän jälkeen yksinkertaisella Visual Basic -pohjaisella ohjelmalla siepattiin kaikki tulenkäytön viestiliikenne ja maalimerkeistä muodostettiin sana ”MOI” harmittomaan paikkaan
- Tämän johdosta Keltainen onnistui suorittamaan maihinnousun ilman, että Sininen sai ammuttua yhtään ainutta meritorjuntaohjusta
- Pieni asia UNOHTUI: tarkistustunnusten käyttö + varmistaminen kuka pyytää liikenneperusteita => iso vaikutus

Paniikin synnyttäminen ”sohaisemalla”

- Netcentric Warfare aikakaudelta 90-luvun alkupuolella
- On ihan normaalia, että kun aktiviteetti/kuorma/liikenne lisääntyy, niin verkoissa/järjestelmissä tulee omituisia hälyjä yms.
- Sitä voi käyttää myös hyväksi paniikin lietsomisessa sohaisemalla => mind games
  - Psykologiset tekijät
  - Vastustajan kykyjen yliarviointi ja omien aliarviointi
- Neljästä fyysisestä lokaatiosta täsmälleen yhtä aikaa sama pitkä ”puppugeneraattori” –sanoma radioverkkoihin => aiheutti hetkellisen verkon ”tukkeutumisen” n. 10-15 s, josta seurasi hetkellinen lumivyöryilmiö verkon toipuessa
- Sai aikaiseksi Sinisellä puolella paniikinomaisen reaktion ”Keltainen on verkoissamme, vaihdetaan liikennöintiperusteet HETI! ” => Sininen sotki ihan itse oman johtamistoimintansa yli 16 tunniksi

Ylireagointi ”hyvässä tarkoituksessa” 9/11

- Object Management Group standardointi
  - Mm. CORBA Middleware, jota käytetään paljon kriittisissä järjestelmissä
  - 9/11 kokous Torontossa ja Pearsonin kenttä oli kuin USS Enterprisen lentokansi…
- Sotilas- ja kriisinhallinnan teknologioiden C4I Domain Task Force kokous 9/13
  - Boeing ja Airbus esittivät, että koska heidän koneidensa ”fly-by-wire” –järjestelmät ovat CORBA Middlewaren päällä, voitaisiin rakentaa komentolinkki, jolla kaapatut koneet voisi ottaa maasta ohjaukseen
  - Ajatus keräsi suurta kannatusta insinöörien ja nörttien joukossa
  - Task Force:n puheenjohtajana ja ainoana upseeritaustaisena totesin kuivasti: ”Ajattelitte sitten rakentaa terroristeille täydellisen asejärjestelmän, ei tarvitse kaapata koneita, komentolinkin hakkerointi riittää!”
  - Tähän USA:n apulaispuolustusministeri tri Vitalji Garber: ”Vain Pentagonin kuolleen ruumiin ylitse, hyvä Hakki kun hoksasit!”
- ”Tie helvettiin on kivetty hyvillä aikomuksilla…”

Palvelualttiuden ja hyväntahtoisuuden väärinkäyttö

- Sattuipa kerran, että A2 Keltainen valtion delegaatio oli käymässä Sinisessä valtiossa
- Vierailun loppumetreillä Keltaisen delegaation yksi avustaja Sinisen avustajalle: ”Kuule, meillä olisi junaliput tässä USB-tikulla, oletko kiltti ja printtaat, kun en ehtinyt lähtiessäni?”
- Ja Sininen hövelisti: ”Tottakai!” ja tikku sisäverkon puolella koneeseen kiinni…
  - Vahinkoa ei edes heti tajuttu Sinisen puolella…
  - Jotta nöyryytys, kettuilu ja kunnon ”mind game” olisi täydellinen, jo vierailun aikaan oli tiedossa Keltaisen delegaation johtajan nimitys uudeksi ulkomaantiedustelupalvelun pääjohtajaksi

Miten inhimillistä tekijää voi pienentää?

- Tietoturvan haastavin päätelaite on homo sapiens
- Kyber-/tietoturva koetaan turhan mystiseksi, jopa pelottavaksi
- Osin turvallisuudesta vastaavat ovat itse syyllisiä luomalla ”kielletään kaikki” ilmapiiriä
- Pitää päästä turvallisuusmyönteisempään kulttuurin
  - Liki liippasi tai lipsahdukset pitää uskaltaa kertoa
  - Aktiivisesti ilmoittaa kaikki havainnot/poikkeamat
  - Käydään tapauksia läpi ”opiksi kaikille” tyyliin
  - Esimerkki: Ilmavoimat
    - Lentoturvallisuuskulttuuri oli II MS:n jälkeen kohtuu retuperällä
    - Järjestelmällinen työ pientenkin poikkeamien ilmoittamiseen
    - Tapausten läpikäynti ja opit

Kiitos !

Profit Consulting Oy
Lars Sonckin kaari 16
02600 ESPOO

www.profitconsulting.fi

Kysy lisätietoja osaamisesta ja palveluista:

Ari Kemppainen, 0400 933 158
Hannu Vähäsaari, 0400 381 985

etunimi.sukunimi@protifconsulting.fi