Ydinvoimalaitos kyberturvallisuuden kohteena

Haasteet, ratkaisumallit ja viranomaisvalvonta

16.10.2013 Mika Koskela

STUK

Säteilyturvakeskus STUK

- n. 350 hengen organisaatio, pääjohtaja Petteri Tiippana
- Keskeisimmät vastuualueet Ydinvoimaitosten valvonta (~110h), Ydinmateriaalien valvonta sekä säteilylähteiden ja säteilyä hyödyntävien laitteiden valvonta
- Selkeä rooli valmiustilanteissa: tarjoaa tietoa ja asiantuntemusta ydin- ja säteilyturvallisuusonnettomuuksissa
- Lainsäädännöllisesti ydinturvallisuus ja säteilyturvallisuusnäkökulma, ei varsinaisesti huoltovarmuusnäkökulma
- Hallintoviranomainen, jonka toimiala ja hyväksymiskriteerit määritelty keskeisimmin ydinenergialaissa/asetuksessa, valtioneuvoston asetuksissa sekä yksityiskohtaisemmin STUKin itsensä asettamissa ohjeissa ja päätöksissä (esim. STUK YVL-ohjeisto)

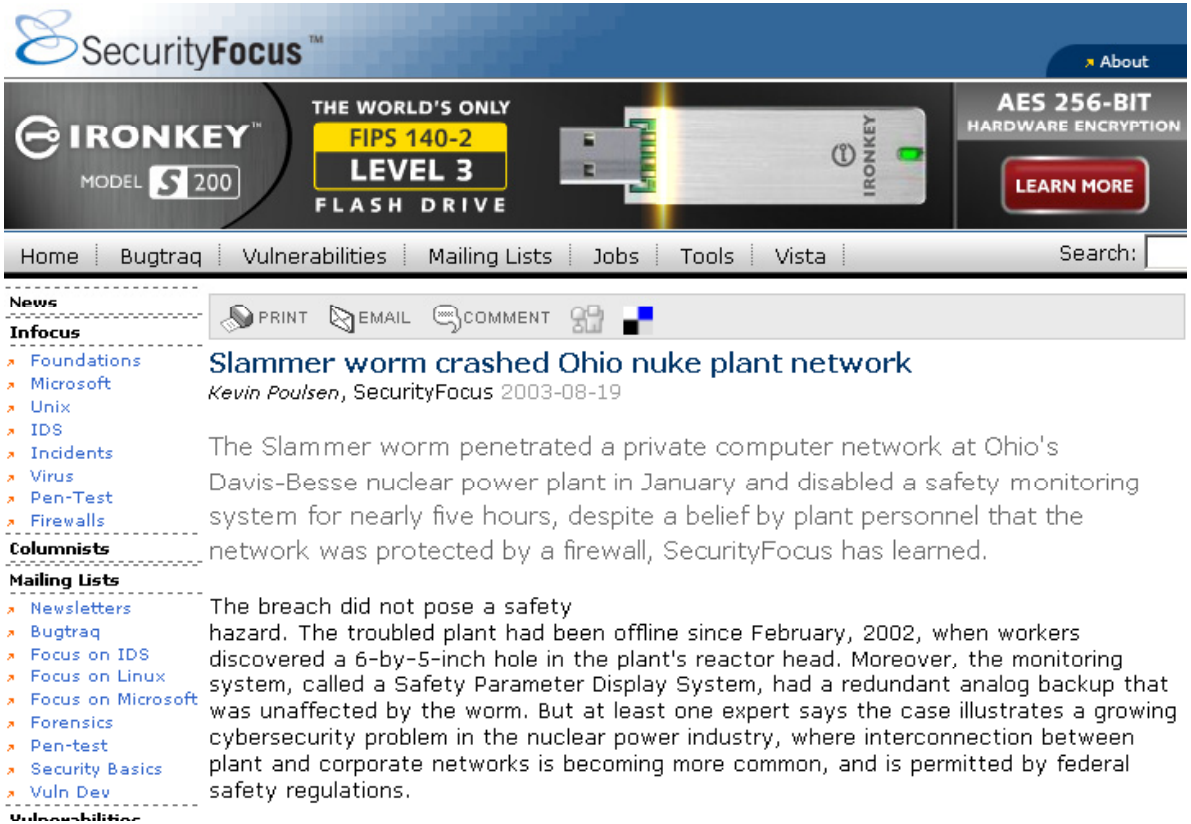
Perusteet

- Kyberturvallisuuden pelikentän peruskäsitteet ovat seuraavat:
  - **Hyökkääjä**, jolla on toiminnallaan tietty **tavoite**
  - **Kohde** jota hyväksikäyttämällä hyökkääjä ajattelee pääsevänä tavoitteeseensa, eli johon toiminta kohdistuu
  - **Puolustaja**, jonka omaisuuteen/hallinta-alueeseen kohde kuuluu, ja jonka toimintaa hyökkääjän toiminta haittaa/voi haitata
- Peli sinänsä on sama mitä ikiaikaisesti on ollut;
  - ammattitaitoisesti suoritettu hyökkäys koostuu tiedustelusta, valmistautumisesta/harjoittelusta, toteuttamisesta ja mahdollisesta vetäytymisestä
  - kybermaailma on ulottuvuus siinä missä maa, meri ja ilma.
- Erona on (tällä hetkellä) puolustajan kannalta epäreilu tasapainotilanne resurssien ja osaamisen kannalta
  - pienilläkin resursseilla voi saada aikaan onnistuneen hyökkäyksen
  - hyökkääjän tarvitsee onnistua kerran, puolustajan on onnistuttava jatkuvasti
  - tarvittava tietotaito on pitkälti avoimesti saatavilla

Ydinvoimalaitos kyberkohteena

- ”Klassinen”, motiivisuuntautunut jaottelu:
  - cybervandalism (tehdään kun kerran pystytään, hauskaa on)
  - cybercrime (raha)
  - cyberterrorism (aate, ei valtiollinen toiminta)
  - cyberwar (aate, valtiollinen toiminta)
- Ydinvoimalaitos on prosessilaitos siinä missä muutkin
  - ydinvoimalaitos = sähköteholliseti iso voimalaitos ”jälkilämpöominaisuudella”
  - lisätekijänä radioaktiivisten aineiden aiheuttama lisäriski…
  - …joka on kuitenkin varsin mitätön verrattuna lisäriskin mahdollistamaan mediaseksikkyyteen informaatiosodankäynnin/mediaterrorismin näkökulmasta
- Vaikutus tulee prosessin kautta, ei (tietoturva)teknologian
- Olennaista ei ole ydinmaailmanlopun hakeminen, vaan pienempikin riittää
  - mediassa ”ydin”- yhdyssanat nostavat helposti kärpäsestä härkäsen

Before Stuxnet – Davis-Besse 01/2003



- Slammer; MS SQL Server ylivuotohaavoittuvuus, joka kuormitti internetiä 2009
- haava julkaistu 04/2002, patchi vähän myöhemmin
- ensin alihankkijan verkkoon, josta laitosverkkoon, josta (palomuurista ohitettua reittiä) valvomo-järjestelmiin → digitaalinen valvomojärjestelmä alas.

B.S. - Wonderware (Invensys) Suitelink 01/2008

digitoday

UUTISLISTA | data | bisnes | mobiili | työ ja ura | tietoturva | tiede ja teknologia | viimpaimet | yhteiskunta

Paikko julkaistiin nopeasti

Voimalaitosten ohjelmistosta löytyi vaarallinen haavoittuvuus

19.5. klo 07:54 Voimalaitosten yleisesti käyttämästä ohjelmistosta löytyi haavoittuvuus Yhdysvalloissa. Terroristit olisivat voineet saada paljon tuhoa aikaan Suitelink-ohjelman aukon avulla.

Core Security-tietoturvayhtiö löysi vaarallisen haavoittuvuuden Suitelink-ohjelmasta. Suitelinkiä käytetään laajalti ohjaamassa voimalaitoksissa, öljynpuhdistamoissa ja tuotantolinjoilla. Terroristit tai krakkerit olisivat voineet pysäyttää ohjelman

Kuva: Pekka Sakki/Lehtikuva

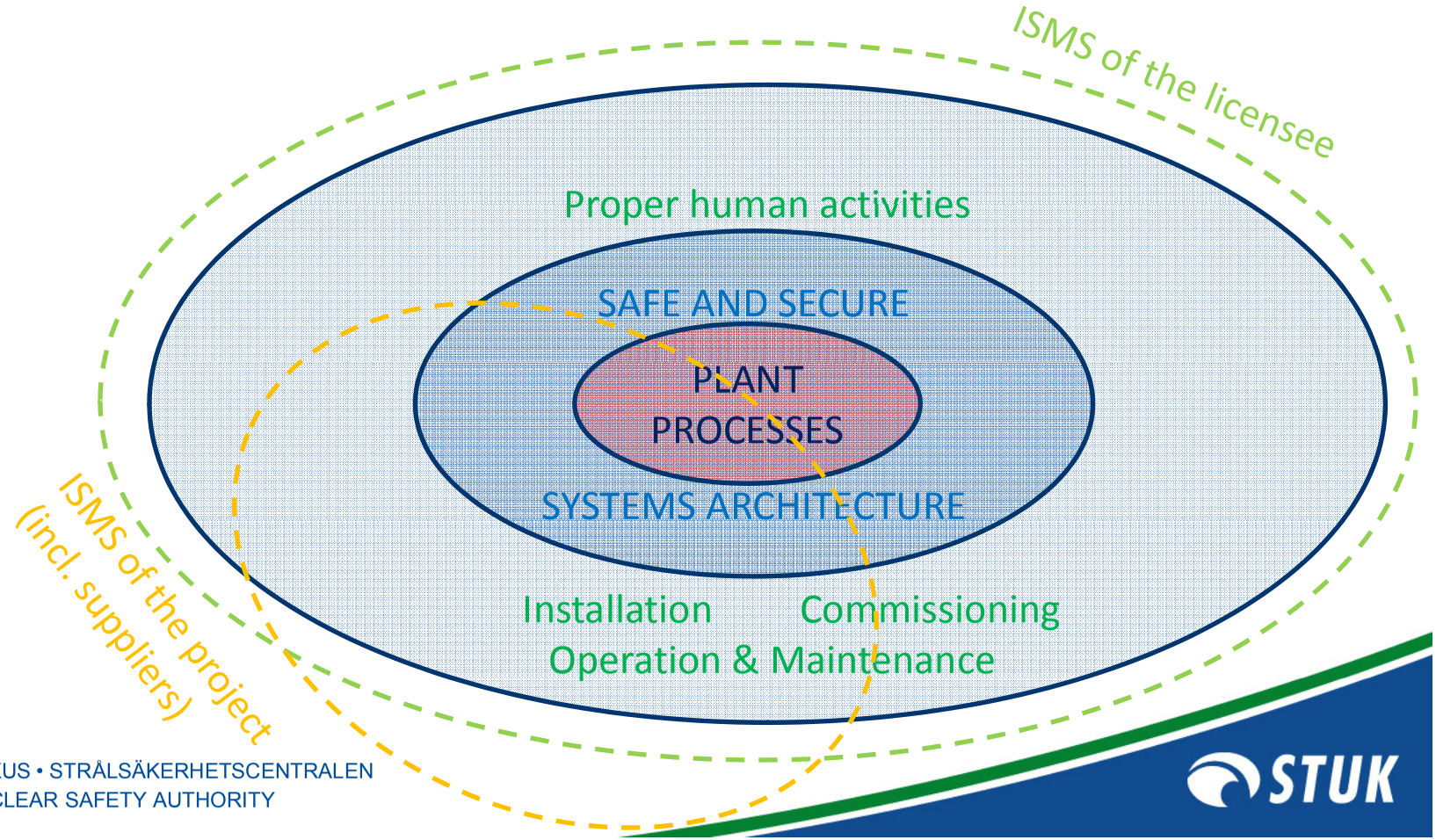
- DoS haava
- Haava sinänsä ei mielenkiintoinen (väärinmuotoiltuun pakettiin kyykkääminen), mutta alla oleva tarina heijastaa hyvin ajan kuvaa ja toimittajien asennoitumista
- http://seclists.org/fulldisclosure/2008/May/95

Stuxnet 2010

- STUXNET oli ensimmäinen julkisesti havaittu cyberase, joka on sekä teknisesti että tarkoitukseltaan uuden sukupolven verkkosodankäyntituote.
  - ensimmäinen fyysisen maailman prosesseihin vaikuttamaan pystyvä haittaohjelma, joka käyttää hyväkseen ICS- järjestelmien heikkouksia
  - kohdennettu verkkosodankäynnin tuote, jonka kohde – uraanin rikastuslaitos Iranin Natanzissa - on asetettu ilmeisen poliittisista pyrkimyksistä (ks. NY Times 1.7.2012)
  - teknisesti edistynyt; käyttää leviämiseen useaa eri haavoittuvuutta, joista osa nollapäivähyökkäyksiä, pystyy piiloutumaan ja päivittymään
  - osa tuoteperhettä, joista myöhemmin havaittu hiljaisempia tiedustelutyökaluja Duqu (hav.2011), Flame (hav.2012).
- Mielenkiintoista itse tekniikan lisäksi oli se miten eri toimijat reagoivat
  - US (ICS) CERT, Siemens, tietoturvayhtiöt, itsenäiset konsultit

Countermeasures

- Ensisijaisesti: prosessin sisäsyntyiseen turvallisuuteen pyrkiminen
- Toiseksi: Robustit järjestelmät (sekä turva että käyttö)
- Kolmanneksi: ISMS:t ja tietoturvallisuuskulttuuri



Ydinvoimalaitosten kyberturvallisuuden valvonta

- STUK valvoo ydinturvallisuutta rauhanajan toiminnan mielessä
- Säännöstöpohja:
  - VNA 734/2008 : Ydinlaitosten turvajärjestelyt
    4§ 4k: Ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa on käytettävä kehittyneitä tietoturvallisuusperiaatteita. Luvaton pääsy ydinlaitoksen suojaus-, ohjaus- ja säätöjärjestelmiin on estettävä
    3§ 2k: Turvajärjestelyjen suunnittelussa on varauduttava muun ohessa siihen, että lainvastaiseen toimintaan saattaa ryhtyä yksittäinen ydinlaitoksella työskentelevä tai ydinmateriaalin tai -jätteen käsittelyyn ja kuljetukseen osallistuva henkilö taikka ulkopuolinen ryhmä tai henkilö, jolla voi olla avustajana laitoksella tai kuljetukseen liittyvässä tehtävässä työskentelevä henkilö. Suunnittelussa on myös otettava huomioon se mahdollisuus, että lainvastaista toimintaa yrittävällä henkilöllä tai ryhmällä on tavanomaisia tai sähkömagneettiseen, kemialliseen tai biologiseen vaikutukseen perustuvia aseita ja räjähteitä sekä sellaista tietoa ja asiantuntemusta, jota ei ole julkisesti saatavilla.
  - Voimassaolevat ohjeet: YVL 5.5 (2002), YVL 5.2 (2004)
  - Kehityksessä oleva ohje STUK YVL A12

Kehitteillä oleva ohje STUK YVL A12

Ohje YVL A.12 Ydinlaitoksen tietoturvallisuuden hallinta L2

Sisällysluettelo

VALTUUTUSPERUSTEET 2

SOVELTAMISSÄÄNNÖT 2

1 JOHDANTO 3

2 SOVELTAMISALA 3

3 TIETOTURVALLISUUDEN HALLINTA 4

3.1 Yleiset vaatimukset 4
3.2 Tietoturvallisuuden hallintajärjestelmä 4
3.3 Asiakirjoja koskevat vaatimukset 6
3.4 Resurssien hallinta 6
3.5 Tietoturvallisuuden hallintajärjestelmän auditoinnit ja katselmukset 6
3.6 Tietoturvallisuuden hallintajärjestelmän parantaminen 7

4 TURVALLISUUDEN KANNALTA TÄRKEIDEN JÄRJESTELMIEN SUOJAAMINEN 8

4.1 Yleiset vaatimukset 8
4.2 Tietoliikenteen ja käyttötoimintojen hallinta ja kontrollointi 8
4.3 Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito 9
4.4 Tietoturvallisuushäiriöiden hallinta 9
4.5 Pääsyoikeuksien hallinta 9
4. 6 Tietoturvallisuuteen liittyvien järjestelmien testaaminen 9

5. SÄTEILYTURVAKESKUKSEN VALVONTAMENETTELYT 11

5.1 Periaatepäätösvaihe 11
5.2 Rakentamislupavaihe 11
5.4 Käyttölupavaihe 12
5.5 Käyttövaihe 13
5.6 Käytöstäpoistovaihe 14
6 Ohjeessa käytetyt määritelmät ja lyhenteet 15

VIITTEET 16

- Ohjeen luonnos L2 kommenteilla sidosryhmillä
- Ei anna varsinaista ”temppulistaa” vaan lähtee riskien tunnistamisesta ja niihin varautumisesta
- Pelkällä ohjeella ei pitkälle pääse; tekniset referenssit oltava hallinnassa

Lopuksi

- Uhkakuvissa on hyväksyttävä realismina teknisesti korkeatasoiset, korkealla tietotaidolla ja resursseilla rakennetuilla työkaluilla mahdollistetut kohdennetut uhat
- Teollisuusautomaatiossa käytettävien ohjelmistojen tietoturvallisuuden taso on se mikä on eikä muutos ole kovin nopea
- Rationaalinen päätöksenteko perustuu cost-benefit ajatteluun. **Riskien/uhkien tunnistaminen** ja niiden arvottaminen on kuitenkin haasteellista.
  - poikkitekninen uhka vaatii poikkiteknistä arviointia ja poikkiteknistä puolustaututumista
  - ihmisen kyky ajatella pienten todennäköisyyksien tapahtumia on varsin puutteellinen
  - mittakaava: laitenäkökulmasta tarkastelu johtaa laitenäkökulman kattavaan ratkaisuun
- Ikuinen tradeoff: tietoa tarvitaan, mutta tietoa ei saisi kertoa
  - vrt. US tiedusteluorganisaatioiden dilemma (Wikileaks). Jotta tiedosta on hyötyä sitä pitää pystyä yhdistelemään ja käyttämään, mutta aina liika tieto ei ole hyvästä
  - ollakseen kyky puolustautua pitää osata ajatella hyökkääjän tavoin => kilpavarustelu on osa evoluutiota
- Ala on biznezz. Profeettoja riittää, ja keskeistä on taito tunnistaa olennainen informaatio massasta
  - keskustelu vietävä ylemmälle tasolle kuin ”tää tuote on parempi kun toi toinen”