

VALVO JA VARAUDU PAHIMPAAN

Erkki Sivonen

Senior Account Manager

Nordic LAN&WAN Communication

erkki.sivonen@lanwan.fi



LAN&WAN

Energy firm cyber-defence is 'too weak', insurers say

By Mark Ward

Technology correspondent, BBC News



YLEISET

JATKUVUUDENHALLINNA
KYSYMYKSET 1-7

1. Johtaminen
2. Toimintasuunnitelmat
3. Henkilöstö
4. Resurssit ja kumppanit
5. Prosessit
6. Mittarit
7. Kyberturvallisuus

UUSI SÄHKÖMARKKINALAKI:
KYSYMYKSET 5.10.-5.17

1. Yhtiön varautumissuunnittelun perustiedot
2. Häiriötilanteiden hallinnan vastuut ja järjestelyt
3. Kriittisiin häiriötilanteisiin ja poikkeusoloihin varautuminen
4. Teknisten resurssien ja järjestelmien käytettävyyden varmistaminen
5. Palvelutuottajien käytettävyyden varmistaminen
6. Toiminta häiriötilanteissa
7. Alueellinen yhteistyö häiriötilanteissa
8. Yhtiön varautumisen mittarit

Sähkömarkkinalain velvoitteet varautumiselle

- **Verkkojen toimitusvarmuuden tason nostaminen (SML 19§)**
- **Verkonhaltijan varautumisvelvoite (SML 28§)**
- **Verkonhaltijan yhteistyövelvoite (SML 29§)**
 - Häiriötilannekuvan kokoaminen
- **Jakeluverkon asiakkaiden varautumisen ohjaaminen (SML 58§)**
 - Ohjeistus viranomaisille ja yrityksille
 - Ohjeistus kansalaisille
- **Häiriötilannekuvan välittäminen (SML 59§)**

Standardeja

- .Teknologiastandardit

- .ISO 27001

- .Säädökset

- .Tietosuojaalainsäädäntö (EU, kansallinen)

- .PCI-DSS

- .Payment Card Industry Security Standards Council

- .HIPAA (US)

- .The Health Insurance Portability and Accountability Act of 1996 USA

- .FedRamp (US)

- BS 7799 (ISO 17799)**

British Standard 7799: Code of Practice for Information Security, josta on julkaistu myös ISO-standardi 17799. BS 7799 on Iso-Britannian standardointi-instituutin julkaisema suositus organisaation tietoturvallisuuden hallintajärjestelmäksi.



TIEDON PIRSTALOITUMINEN

LAN&WAN

VARAUTUMISEN JA VALVONNAN POSITIO

LIIKETOIMINNALLE TÄRKEÄ



LIIKETOIMINNALLE VÄHEMMÄN TÄRKEÄ

Kokonaisvaltainen valvonta

IT-infra

Tuotanto-
järjestelmät

Kiinteistö-
järjestelmät

Tietoturva

NÄIN SE RAKENTUU

CASE: **FINNAIR**

KÄYTTÄJÄ

LAITE

YHTEYS

- Internet
- Lähiverkko
- Langattomat yhteydet
- Operaattoriyhteydet

SUOJAUS

- Käyttäjän tunnistaminen
- Laitteiden suojaus ja hallinta
- Yhteyden suojaus ja hallinta
- Tiedon ja palvelun eheys ja suojaus

SEURANTA

- Palvelun käytettävyys
- Trendin seuranta
- Valvontatieto
- Analyysi
- parannusehdotukset

PALVELU (sovellus, portaali, ohjelmisto)

TIETO, METADATA, BIG DATA, "ARVOPÄÄOMA"

**TIETOTURVAUHKKA VOI
OLLA LÄHEMPÄNÄ KUIN
USKOTKAAN**



Joka päivä uusia uhkia

Kyberturvallisuus julkaissut varoituksen sisällönhallintajärjestelmän haavoittuvuudesta

21.11.2014 klo 08:28

Wordpress on suosittu www-julkaisujärjestelmä. Sitä käytetään yleisesti. Ohjelmistosta on löydetty vakava haavoittuvuus. Haavoittuvuus vaikuttaa sisällönhallintaan ja viestintään. Haavoittuvuus on löydetty joulukuun alkuun mennessä.

Julkaisujen sisällönhallintaan tarkoite-
vakava haavoittuvuus. Haavoittuvuus
lukemisen, m...

Julkaisu: 3.12.2014 11:45

Viestintävirasto on suositellut käyttäjien välttämästä...

TIETOTURVA F-Securen
salasanoista, lapsen ti...

F-Securen tutkimusjohtaja
Reddit-verkkosivustolla av
Kyselijät esittivät kysymy...

Tietoturvagurua tentattiin
chatista kiinnostavimmat j...

K: Mitä ihmiset tekevät tietoturvasyste...

MH: Käyttävät Internet E...

K: Mikä on analysoimistasi monimutkaisin ja miksi?

MH: Stuxnet. Regin. Rutla. Heillä on paljon rikollisia pa...

Mediuutiset

ETUSIVU Keskustelut Työpaikat » Tapahtumat Yhteystiedot

Viikon uutiset Uutisarkisto Kirjat Rytmihäiriö Sairaalahierailut Sa...

Hyvä juttu | Lähetä | Tulosta | A | A | Facebook | Twitter | +

TIETOTURVA Erpo Pakkala, 11.3.2015, 15:03

Virus livautti potilastietojärjestelmään - Varsinais-Suomen sairaanhoitopiiri kielsi Facebookin käytön

Varsinais-Suomen sairaanhoitopiiri havaitsi tietoverkossaan tietokoneviruksen viime perjantaina ja tämän viikon maanantaina. Virus pääsi verkkoon kummassakin tapauksessa yhden työaseman kautta.

Viruksen epäillään päätyneen työasemalle Facebook-sivuston ja Internet Explorer -selaimen kautta ja siksi Facebookin käyttö on varoitettiin toistaiseksi kielletty ja pääosin estettykin sairaanhoitopiirin tietoverkossa.

Työasemat paikallistettiin nopeasti ja otettiin pois käytöstä, mikä esti viruksen leviämisen muihin työasemiin. Virus ehti vahingoittaa potilastietojärjestelmän kutsukirjepohjia ja niiden liitteitä sekä yleisellä levyalueella noin 20 000–30 000 tiedostoa.

Viruksen takia potilaiden suunniteltuja kutsukirjeitä ei voitu lähettää useaan tuntiin perjantaina sekä vajaaseen tuntiin tiistaina. Kirjepohjia ja -liitteitä on voitu korjausten jälkeen taas käyttää normaalisti.

Virus oli tyypiltään niin sanottu Cryptolocker-haittaohjelma, jollaisia on parhaillaan liikkeellä paljon eri puolilla maailmaa. Aktivoidun haittaohjelman salaa tiedostoja sekä saastuneen koneen paikallisilla levyasemilla että siihen kytkettyneillä verkkolevyasemilla. Ohjelma vaatii kohteeltaan maksua salauksen purkuavainten toimittamisesta. Sairanhoitopiiri ei maksuun suostunut.

Yleisellä levyalueella sijaitsevat vahingoittuneet tiedostot on korvattu varmuuskopioilla.

– Tällä kertaa selvittiin potilashoidon näkökulmasta vain kutsukirjeiden lähettämisen viivästymisellä, eivätkä potilastiedot olleet vaarassa, toteaa sairaanhoitopiirin tietohallintoylläkäri **Pirkko Kortekangas** tiedotteessa.

ta löytyi tietokonevirus
o-laite on riski"

KIMMO TASKINEN HS



oittuvuus
elainistunnon

äyksen avulla

löydetty haavoittuvuus mahdollistaa
sen purkamisen, jos hyökkääjä pääsee
an uhrin ja palvelimen välistä

lynnettävästä SSL 3.0 -salausprotokollasta on
ihdollistaa salatun tietoliikenteen osittaisen
dle"-nimen saanut haavoittuvuus koskee
Erittäin harva selain tai verkkosivu hyödyntää
utta edelleen suurin osa tukee sitä taaksepäin
ksi.

uu siihen, että selainliikenne pakotetaan
ytokollaa uudempien TLS-protokollien sijaan.
s. välimiesasemaa (Man-in-the-Middle), jossa
n ja muokkaamaan uhrin ja palvelimen välistä
ie saattaa syntyä esimerkiksi suojaamatonta
essä.

Tietoturvauhka isossa organisaatiossa

Joka **viides sekunti** havaitaan uusi tuntematon tietoturvauhka

Joka **minuutti** joku käyttäjä selaa jotain haitallista sivustoa

Joka **27. minuutti** käyttäjä lataa tuntemattoman haittaohjelman omalle koneelleen



Tiedot perustuvat tietoturvayhtiöiden tekemiin tutkimuksiin vuosien 2012-2014 aikana.

Security Operations Center



Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

Create account Log in

Article Talk

Read Edit View history

Search

Information security operations center

From Wikipedia, the free encyclopedia
(Redirected from Security operations center (computing))



The **neutrality of this**
until the dispute is resolved

"enterprise information systems"

do not remove this message

An information
desks and

"monitored" "assessed" "defended"

sites, applications, databases, data centers and servers, networks,

Contents [hide]

- Objective
 - 1.1 Regulatory requirements
- Alternative names
- Technology
- People
- Organization
- Facilities
- Process and procedures
- See also
- References

Objective

A SOC is
manages incidents for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigate
applications to identify a possible cyber-attack or intrusion (event) and determine if it is a real, malicious threat (incident), and if it could

"detection"

"containment"

"remediation"

An SOC

Havainnointi tuottaa tapahtumia ..

LAN&WAN LANmanage

Kirjaudu ulos

Pasanen Juha

Nordic LAN&WA... ▼

 Suomi ▼



Palvelut

Valvonta

Raportit

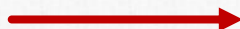
Hallinta



Etusivu » Valvonta

TIETOTURVAHÄLYTYKSET

	08.08.2014 12:53	Low Virus Incident
	13.08.2014 10:33	Low Bot Incident
	18.08.2014 08:46	Low Bot Incident
	21.08.2014 16:14	Low Bot Incident
	21.08.2014 16:19	Low Bot Incident
	27.08.2014 09:56	Low Bot Incident
	27.08.2014 10:27	Low Bot Incident



Name: Bot Incident

Severity: Low

Category: Threat Prevention

DetectedBy: 192.130.30.236

ProtectionName: Trojan-Banker.Win32.Zeus.CL

MalwareAction: P2P communication with Botnet

Source-IP: 172.16.17.197

Destination-IP: 172.16.23.255

Event Id: EN12320809

MsgId: 53980493

Kaikki tietoturvahälytykset, klikkaa tästä

Kaikki tietoturvahälytykset, klikkaa tästä

MsgId: 53980493

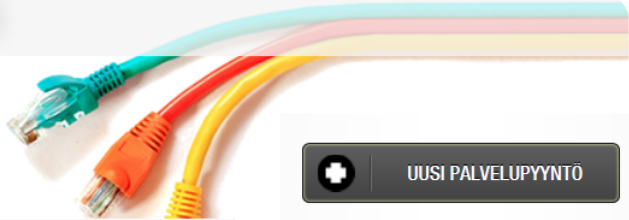
Event Id: EN12320809

08.08.2014 10:53 Low Bot Incident

08.08.2014 09:28 Low Bot Incident

.. jotka käsitellään ennalta suunnitellun prosessin mukaan

 [Palvelut](#) [Valvonta](#) [Raportit](#) [Hallinta](#)



[Etusivu](#) » [Palvelut](#) » [Palvelupyynnöt](#) » [INC106450] Huoltopyyntö

CRITICAL BOT INCIDENT

Tila:	Suljettu	Tyyppi:	Huoltopyyntö
Palvelu:	LANsafe Palomuuuri	Palvelutaso:	PL1
Pyytjä:	Service desk	Hoitaja:	Jussila Ville
Avattu:	15.07.2014 14:30	Päivitetty:	14.08.2014 09:28
Linkitykset:			
Sähköposti ilmoitus:	Lähetys: Ei lähetetä Sähköposti: servicedesk@lanwan.fi		
Liitetiedostot:			

15.07.2014 14:30
Service desk

Name: Bot Incident
Severity: Critical
Category: Threat Prevention
DetectedBy: 213.255.191.13
ProtectionName: Operator.Pua.dzn
MalwareAction: Communication with C&C site
Source-IP: 10.100.0.64
Destination-IP: 50.97.62.154
Event Id: EN02762829
MsgId: 9925850

 Hälytys 39

 Varoitus 17

 Kunnossa 1470

 UUSI PALVELUPYYNTÖ

Tietoturva ei ole välineurheilua

- 80 % tietoturvakustannuksista on työtä
- Tietoturvan toteuttamiseen tarvitaan laaja-alaista osaamista ja riittävää resursointia
- Palomuuripalvelu ei ole sama asia kun SOC
- SOC:ia ei voi korvata laitteilla



LAN&WAN



5/13/2015

LAN&WAN

KIITOS

Nordic LAN&WAN Communication Oy
Erkki Sivonen & Kari Salmela
Senior Account Manager
erkki.sivonen@lanwan.fi

KYSYMYKSIÄ?

