nixu cybersecurity.

MITEN TOTEUTAN TIETOSUOJAN TEHOKKAASTI?

Teknologiateollisuus: Koulutuksia tietoturvasta 2017
13.2.2017 #turvallaan2017
@nixutigerteam

SISÄLTÖ

Petri Kairinen, toimitusjohtaja, Nixu Oyj (@kairinen)

Kira Ahveninen-Kuha, lakimies/tietosuoja-asiantuntija, Nixu Oyj (@kira2fish)

- Tietosuoja mahdollistajana / Petri
- Miten toteuttaa tietosuojaa liiketoimintalähtöisesti / Kira
- Käytännön esimerkkejä teknologia-alan yritysten tilanteesta / Kira
- Miten tietomurto havaitaan ja miten toimitaan oikein tilanteessa? / Petri

WE KEEP THE DIGITAL SOCIETY RUNNING

13.2.2017

nixu

Tietosuoja mahdollistajana

DIGITAALINEN TULEVAISUUS, CASE: KONE

- https://www.youtube.com/watch?v=Ea2drPIHv8I

Tulevaisuudessa hissit tietävät yhä enemmän käyttäjistä ja voimme tuoda uusia palveluita, jotka on tarkoitettu nimenomaan käyttäjille.

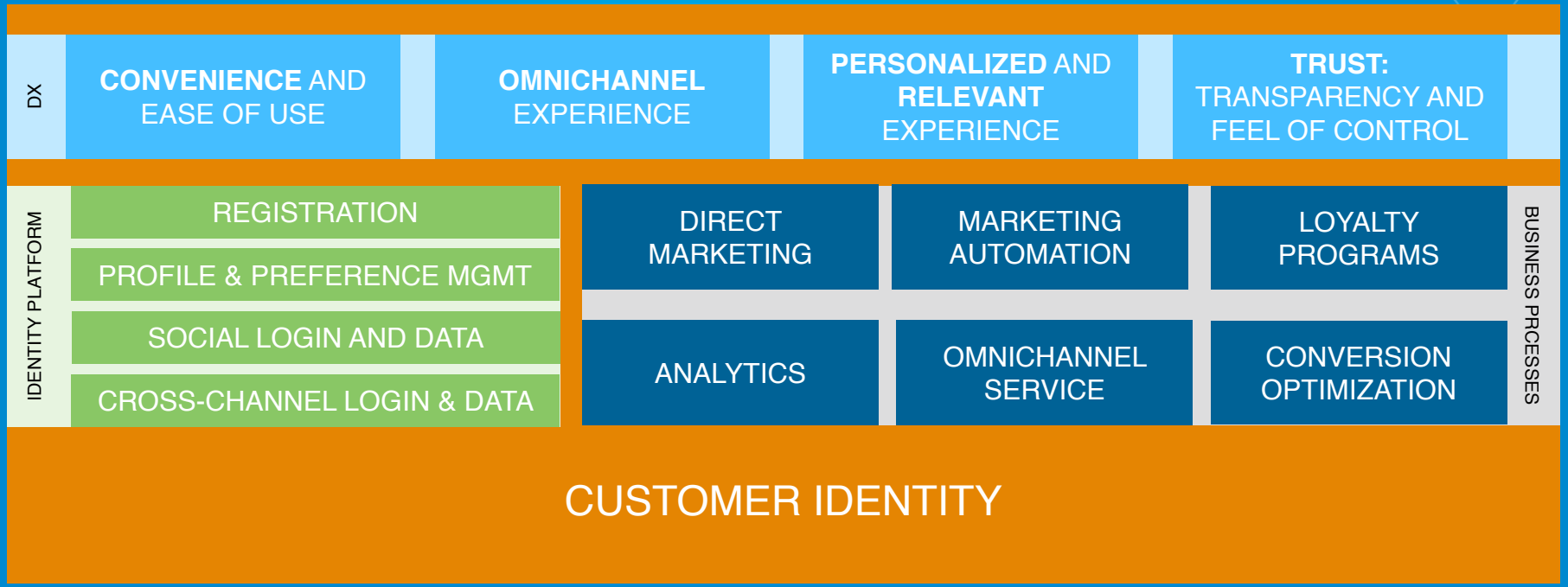
- Henrik Ehrnrooth, Kone, HS 9.2.2017

TRENDEJÄ

nixu

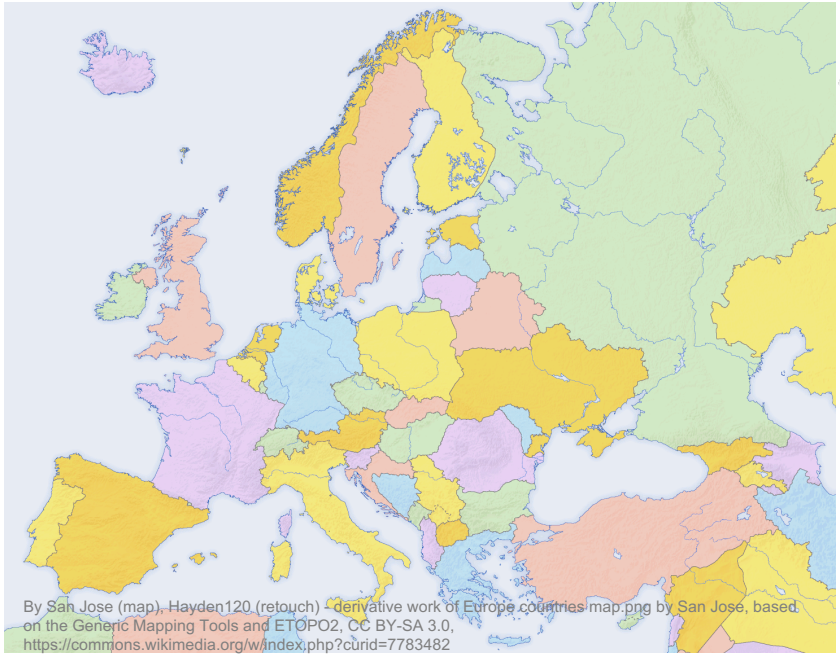
Digitaalinen liiketoiminta tarvitsee dataa, ja kuluttajat vaativat parempia palveluita vastineeksi datastaan.

DIGITAALINEN IDENTITEETTI

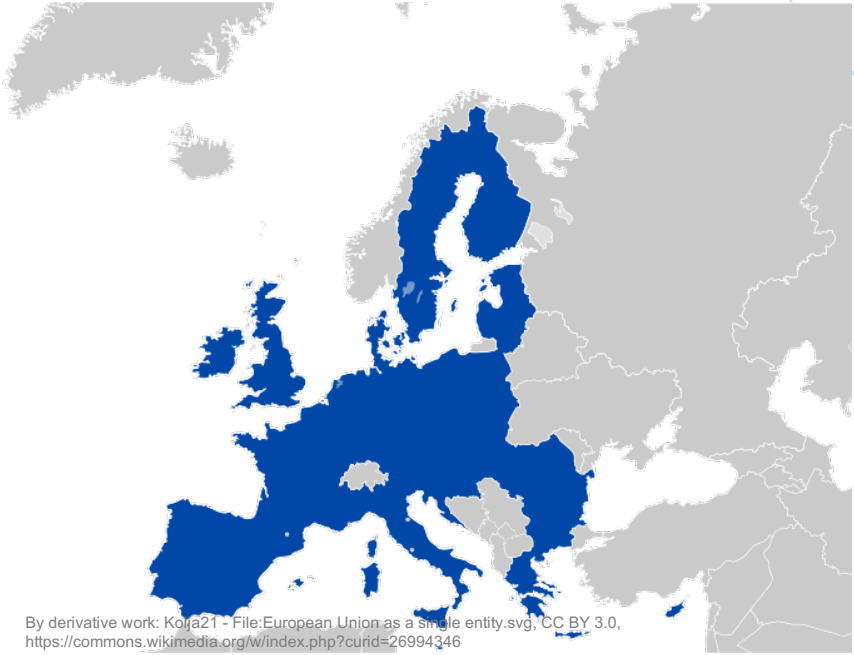


nixu

GDPR: KUMMAN MARKKINAN HALUAT?



By San Jose (map), Hayden120 (retouch) - derivative work of Europe countries map.png by San Jose, based on the Generic Mapping Tools and ETOPO2, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=7783482



By derivative work: Kolja21 - File:European Union as a single entity.svg, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=26994346

Tietosuojan toteutus liiketoimintalähtöisesti

13.2.2017

nixu

TheRealDeal

All | I want to order ... | Go

0 4.0000 / BTC 4.0000

In stock.

Postage Option

Qty: 0

Buy It Now

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

Favorite | Question

Details | Feedback | Return Policy

Description

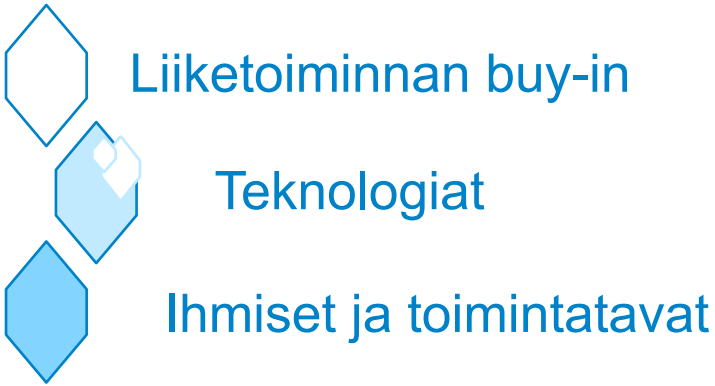
```
68,743,269 Lines of data which were taken from the Neopets databse in March 2014.

Lines include;
Username;pass;email;DoB;country;Gender;IP;name.

Full data in plain text, no passwords are encrypted - Great for reuse.

 Note: not all recods have full data(etc DoB,Name)
```

nixu

TIETOSUOJA-COMPLIANCEN JALKAUTTAMINEN

Osoitusvelvollisuus

Muutosjohtaminen



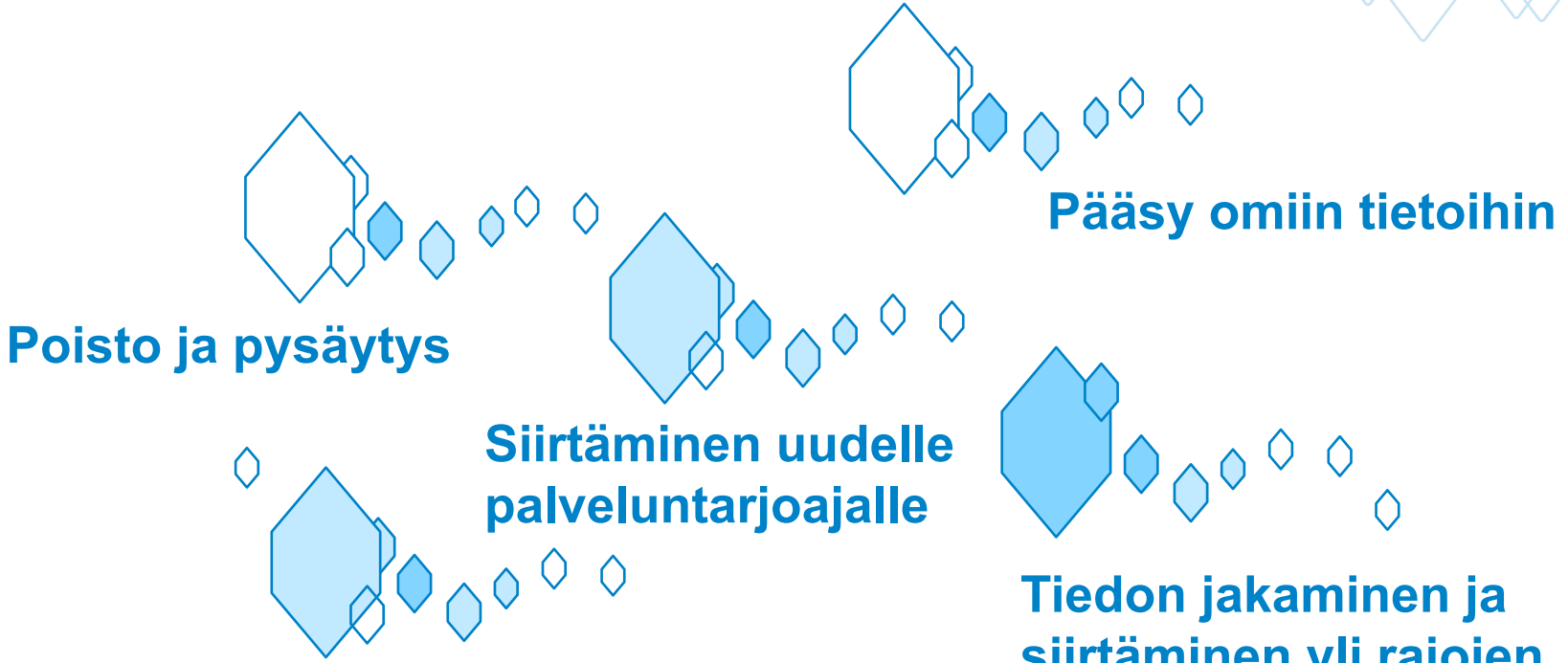
TIETOSUOJAMATURITEETIN ERI VAIHEET

nixu

Teknologiavaatimukset

TEKNOLOGIAN JA TIETOSUOJAN LIMITTYMINEN

TIETOJÄRJESTELMIIN KOHDISTUVAT VAATIMUKSET



nixu

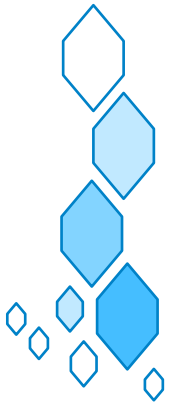
Kuinka suhtautua tietosuojariskeihin?

nixu

LÄHTÖKOHTIA TIETOSUOJARISKIEN HALLINTAAN

- Uhkamallinnus
- Valinta: asetetaanko riskille kontrolli vai mitigoidaanko
- Vaikutuksenarviointi – metodiikan hyväksikäyttäminen ja riskiperusteinen toimintatapa
- Johda teknologiaa ja ICT-hankintoja tietosuoja ja tietoturva huomioiden
- Data Protection by Design – malli kehitystoimintaan
- Määrittele turvalliset tavat poistaa tietoa pysyvästi
  - Seuraa jäännösriskiä
- Panosta pääsyn- ja käyttövaltuuksien hallintaan
- Panosta tiedonhallintaan ja eheyteen
- Käyttäjä keskiössä

DATA PROTECTION BY DESIGN – MALLIN RÄÄTÄLÖINTI



1. Tietosuojavaatimukset, tietosuojan tarkastuspisteet, vastuullinen design
2. Vaikutusten arviointi tietosuojaa koskien
3. Dokumentointi ja Quality Gate/KPI -suunnittelu
4. Laadunvarmistus ennen julkistamista

Tietosuojan ja tietoturvan yhtymäkohtia

Tietosuoja-asetuksen artikla 32: käsittelyn turvallisuus

13.2.2017

nixu

TIETOTURVA JA KYBERTURVA TIETOSUOJAVELVOITTEINA

Artikla 32: kryptaaminen, organisatoris-hallinnollinen tietoturva, perinteiset tietoturvaperiaatteet

- Eheys
- Luottamuksellisuus
- Saatavuus
- Uutena: pseudonymisoinnin käyttö

TIETOTURVA JA KYBERTURVA TIETOSUOJAVELVOITTEINA

Iso-Britannian tietosuojaviranomainen ICO antoi telecom-yritys TalkTalkille 400 000 punnan sakot *tietosuojalainsäädäntöön perustuen tietoturvallisuuden laiminlyönnistä* lokakuussa 2016

- Hakkerit pääsivät käsiksi yli 150 000 asiakkaan tietoihin (nimet, osoitteet, syntymäajat, puhelinnumerot ja sähköpostiosoitteet; lisäksi yli 15 000 asiakkaan pankkitilitietoihin päästiin käsiksi)
- *Hakkerit pääsivät hyökkäämään SQL-injektion kautta, joka on hyvin tunnettu ja helposti suojauduttavissa oleva haavoittuvuus*
- *Erityisen moitittavaa tapahtuneessa oli TalkTalkin oma huolimattomuus tietoturvan ylläpidossa*

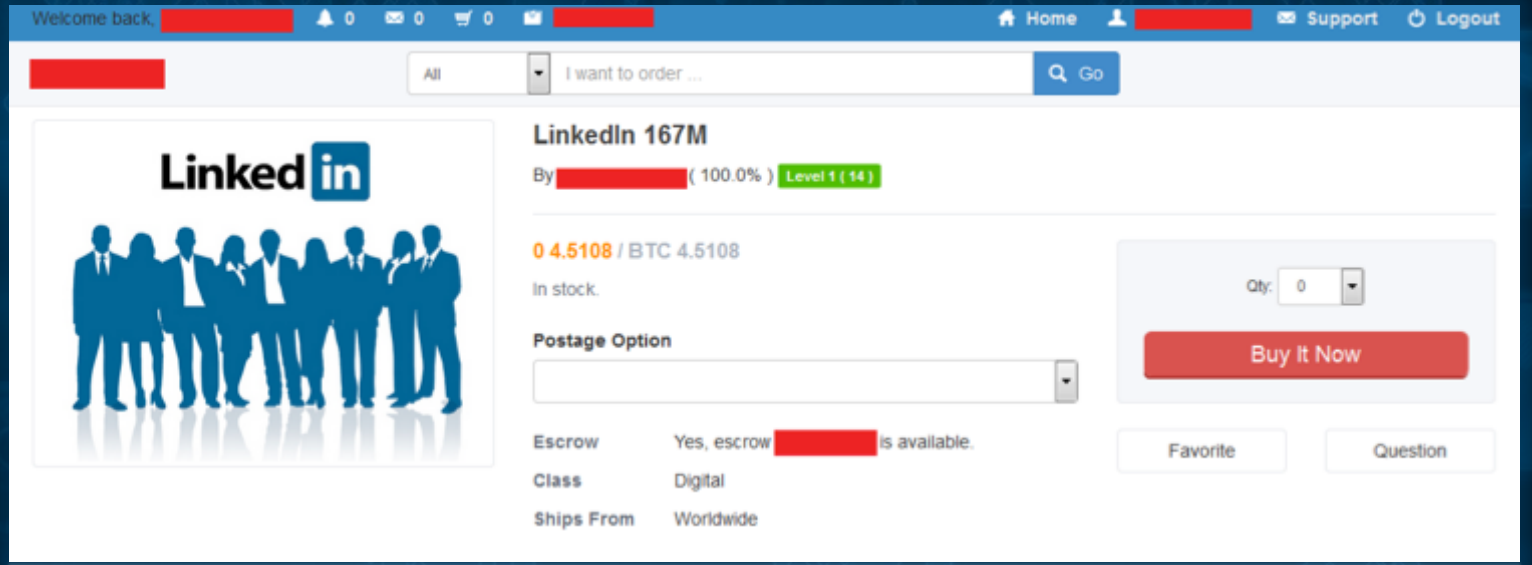
TIETOMURTOIHIN VARAUTUMINEN TIETOSUOJAVELVOLLISUUTENA

- Rekisterinpitäjällä pitää olla ***kyky havaita*** mahdollinen tietoturvaloukkaus
- Tietoturvahyökkäys, tietovuoto, vahinko tai vuosia sitten tapahtunut virhe
- Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä *ilman aiheetonta viivytystä*, ja mahdollisuuksien mukaan 72 tunnin kuluessa
  - Tietyin edellytyksin valvontaviranomaiselle
  - Tietyin edellytyksin rekisteröidylle henkilölle

MITEN TIETOMURTO HAVAITAAN JA MITEN TOIMITAAN OIKEIN?

13.2.2017

nixu



nixu

KUN TIETOMURTO TAPAHTUU

206 päivää

Mediaaniaika tietomurron havaitsemiseen.

69 päivää

Mediaaniaika tietomurron haltuunsaamiseen havaitsemisesta

79 %

Tietomurroista johtuu sisäpiiriläisen väärinkäytöksestä

nixu

Sources: Verizon Data Breach Investigation report 2015, 2015 Cost of Data Breach Study: Global Analysis. Ponemon Institute.

PUOLUSTUKSESTA PALAUTUMISEEN

Valmius

Vulnerability Management

Threat Intel

Operointi

Advanced Cyber Defense

Security Operations Center

Palautuminen

Digital Forensics

Insurance

MITÄ TAPAHTUI?

KUINKA PALJON MENETETTIIN?

MITEN VIESTIMME?

KUINKA NOPEASTI VOIMME PALAUTUA?

nixu

MITÄ MUISTAA?

1. Aloita helpoista voitoista
2. Suunta kohti design for privacy -ajattelua
3. Havainnoi ja varaudu murtoon

KYSYMYKSIÄ?