AWS Sertifikoinnit

Harri Kauhanen, Futurice

http://aws.amazon.com/security/#certifications

- PCI DSS Level 1
- ISO 27001
- SAS 70 Type II
- HIPAA

PCI DSS Level 1

- “Säilytä ja siirrä maksukorttitietoja huolella”
  - vaatii tietovarastojen ja verkkojen jatkuvaa testaamista ja tietoturvapolitiikan ylläpitoa
- Ei ole “PCI sertifikoitu” (maksutapahtumien käsittely) → Saatat tarvita oman PCI sertifikaatin
- VISA/MasterCard/etc. haluaa tätä (ainakin isoilta) palveluntarjoajilta (physical infrastructure service providers)
- EC2, S3, EBS, VPC

ISO 27001

- “Säilytä dataa huolella”
  - Ei suoraan määrittele MITÄ tietoturvauhat ovat...
  - ...vaan vaatii tunnistamaan ne sekä systemaattista toimintaa jatkuvasti muuttuvia tietoturvauhkia vastaan
- “Jotain” täältä: ISO 27002 best practice guidance
  - *"We don’t disclose every control we have in place, but of course we did consider all relevant guidance documented in 27002 as applicable to our scope covering AWS infrastructure, data centers, and services including EC2, S3, and VPC. As part of the certification process our auditors validated that we addressed all aspects of the 27002 guidance appropriate for our systems and services."*
- EC2, S3, VPC

SAS 70 Type II

- “Asiakkaiden dataa seurataan/kontrolloidaan systemaattisesti”
  - Standardin taustalla rahaliikeen transaktioiden varmistaminen
  - Yrittää sanoa “se että käytämme tätä alustaa (3. osapuolena) palvelun X toteutuksessa ei ole riski”
- AWS palveluita ei ole eritelty

HIPAA

- HIPAA = Yhdysvaltain hallinnon säänöstö siitä miten potilastietojen yksityisyys ja tietoturva voidaan varmistaa
- AWS:llä ei ole “HIPAA sertifikointia”
  - Whitepaper, jossa kerrotaan miten HIPAA-vaatimukset täyttävä palvelu rakennetaan AWS:n päälle