Virtualios infrastruktūros sauga

Debesų kompiuterijos sauga

Debesų kompiuterija

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. (*Wikipedia*)

Debesų kompiuterija teikia paslaugas t.y.:

priėjimą prie bendro pobūdžio verslo aplikacijų ir skaičiavimo resursų per web naršykles (pvz. Google Docs), kai programinė įranga ir duomenys saugomi nutolusiame duomenų centre.

Debesų kompiuterijos resursų tipai:

- Privatūs (organizacijos ribose)
- Vieši (prieinami bet kuriam vartotojui)
- Mišrūs (organizacijos/privačių ir viešų resursų sąjunga)

Istorija

1997 prof. R.Chelappa pirmasis pavartojo sąvoką „Cloud computing“, nors tokius principu veikė mainframe tipo kompiuteriai dar ~1960 m.

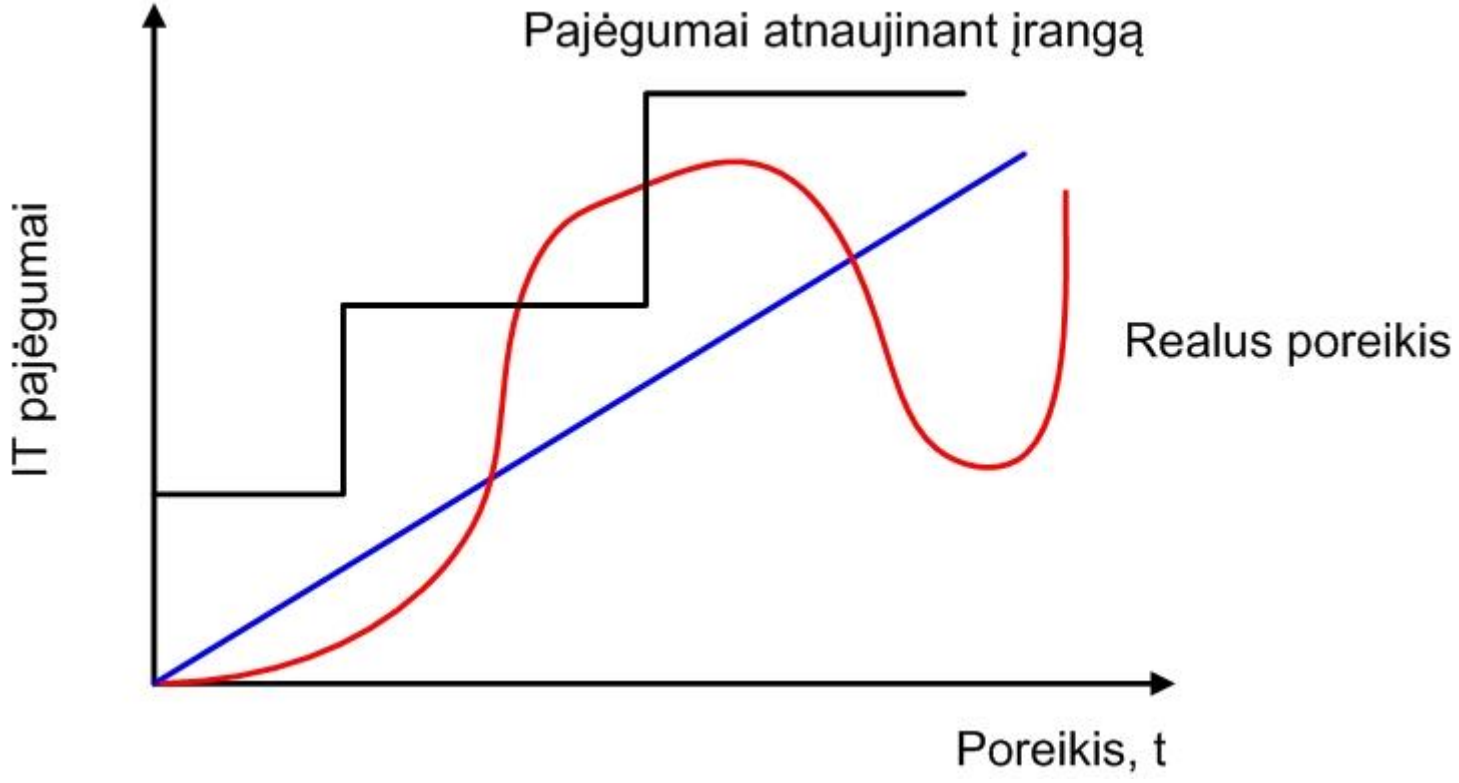
1999 m. Salesforce.com tapo pirmąja svetaine siūlančia programinę įrangą internetu.

2002 m. Amazon pristatė savo „Elastic cloud computing“ (EC2) paslaugas t.y. virtualių mašinų nuomą.

2007 m. Salesforce.com persivadinusi į Force.com pradėjo siūlyti verslo aplikacijas internete.

2008 m. prisijungė Google Apps, Microsoft Azure, Apple iCloud.

Infrastruktūros naudojimas

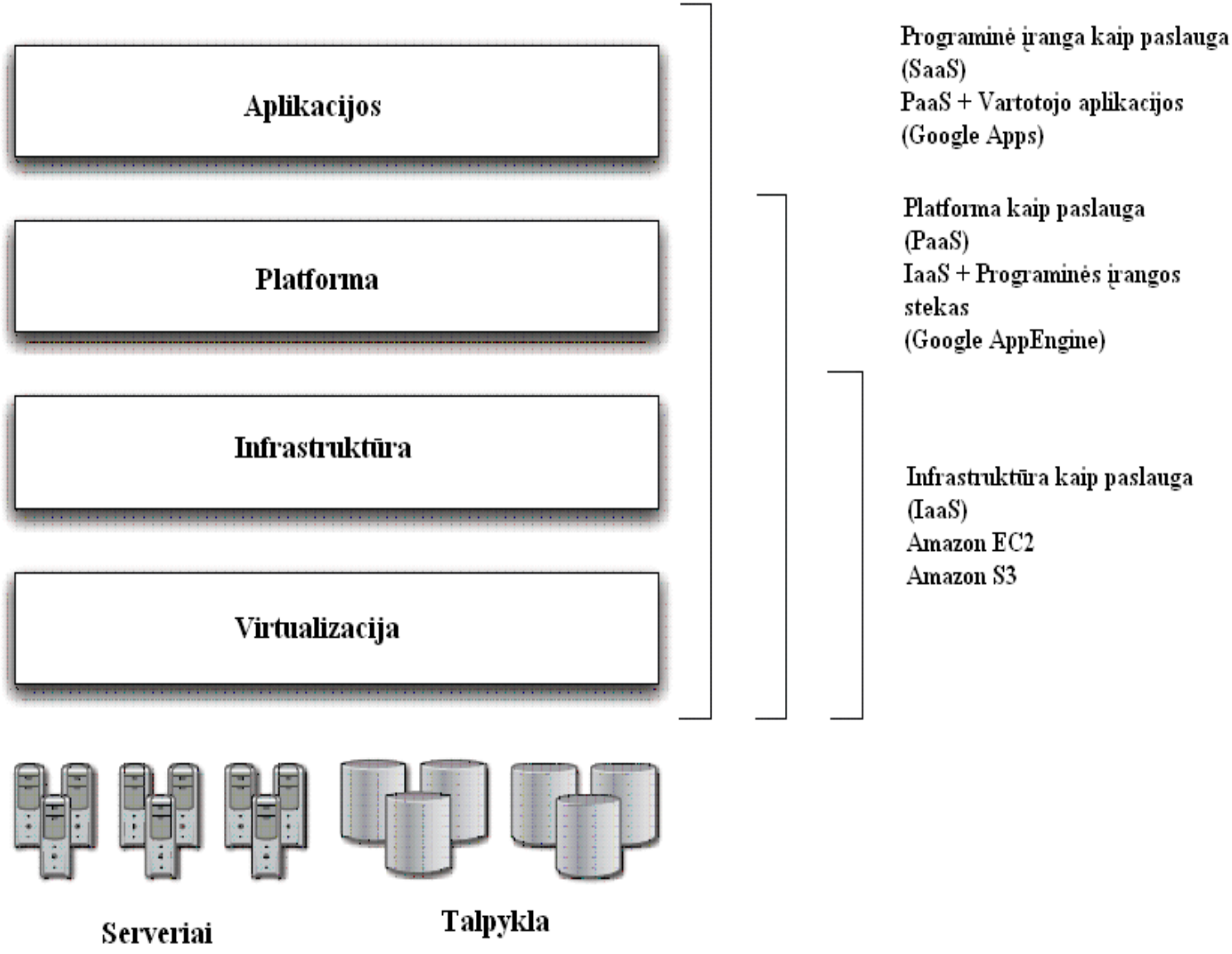


Kada tikslinga naudoti debesis?

Debesų kompiuteriją tikslinga naudoti kai:

- IT resursų poreikis yra nenuolatinis (naudojama – nenaudojama)
- IT resursai turi neperiodinius išaugančių pajėgumų pikus
- Ciklišk ai kinta IT resursų išaugančio pajėgumo poreikis
- Neprognozuojamas IT resursų augimo poreikis

Cloud computing struktūra



Saugos rizikos

Debesų kompiuterijos saugos rizikos:

- IT saugos ir duomenų kontrolės perdavimas trečioms šalims
  - Tenka pasitikėti SLA
- Prieigos kontrolė
  - Autentifikacija + autorizacija
- Infrastruktūros, duomenų izoliavimas (gest-hopping-attack)
- IT infrastruktūros perkėlimas gali būti nesuderintas tarp skirtingų tiekėjų (pririšimas prie paslaugų tiekėjo)
- Duomenų savininko problema
- Nesaugus arba nevisiškas duomenų sunaikinimas
- Įstatyminė bazė duomenų atžvilgiu skirtingose šalyse skiriasi.

Saugos standartai

Gerai žinomi ir plačiai naudojami saugos standartai (ISO 2700x, COBIT ir t.t.) nėra pritaikyti debesų kompiuterijos infrastruktūrai.

Dokumentai, kurie kalba apie debesų kompiuteriją.

- *Cloud computing:Benefits, Risks and Recomendations for Informaction Security*. ENISA (Europenian Network and Information Security Agency).
- *Security Recommendations for Cloud Computing Providers*. German Federal Office for Information Security.
- *Security Guidance for Critical Area of Focus in Cloud Computing*. Cloud Security Alliance.
- National Institute of Standards and Technology dokumentai.

Cloud Security Alliance

Security Guidance for Critical Area of Focus in Cloud Computing – tai saugos rekomendacijų rinkinys debesų kompiuterijai (14 dalių).

1. Architektūros pagrindai – pateikiami debesų kompiuterijos modeliai ir platformos.
2. Valdymo ir įmonių rizikos vadyba
3. Teisinių klausimų vadyba
4. Atitiktis ir auditas
5. Informacijos valdymas ir duomenų sauga
6. Įvairiapusis pasiekiamumas
7. Tradicinė apsauga ir verslo tęstinumo valdymas

Cloud Security Alliance (tęsinys)

8. Duomenų centrų operacijų sauga
9. Programinės įrangos sauga
10. Šifravimas ir raktų valdymas
11. Identifikacijos ir prieigos valdymas

NIST

NIST dokumentai:

1. Recommended Security Control for Federal Information Systems and Organizations.
2. Guidelines on Security and Privacy in Public Cloud Computing.

Dokumentų dalys

1. Atitiktis
2. Pasitikėjimas
3. Achitektūra
4. Tapatybės ir prieigos valdymas
5. Programinės įrangos izoliavimas
6. Prieinamumas

Saugos reikalavimai DK

Apibendrinus saugos standartuose pateiktas rekomendacijas, sudarytas saugos reikalavimų sąrašas.

1. **Infrastruktūros saugos užtikrinimas**

    1.1 Procesų dokumentavimas, siekiant nustatyti saugos grėsmes

    1.2 Atsakomybių priskirimas ir valdymas

    1.3 Pakeitimų valdymo sistema

    1.4 Saugos auditavimas

    1.5 Informacijos saugojimo ir tvarkymo politika

Saugos reikalavimai DK

2. **Operacinių sistemų sauga**
    - 2.1 Operacinių sistemų saugos politika
    - 2.2 Atnaujinimų ir pakeitimų valdymas
    - 2.3 Konfigūracijų kontrolė ir valdymas
3. **Duomenų sauga**
    - 3.1 Klientų duomenų izoliavimas ir sauga
    - 3.2 Visiško duomenų sunaikinimo garantijos
    - 3.3 Kliento duomenų atskyrimas
    - 3.4 Atsarginių kopijų proceso valdymas
    - 3.5 Duomenų apsauga pagal šalies, kurioje jei fiziškai yra, įstatymus

Saugos reikalavimai DK

4. **Fizinė sauga**
    - 4.1 Dviejų lygių autentifikacija
    - 4.2 Vaidmenis pagrįsta valdymo kontrolė (RBAC)
    - 4.3 Centralizuota raktų ir slaptažodžių saugykla
    - 4.4 Monitoringas ir registravimas
5. **Programinės įrangos sauga**
    - 5.1 Programų izoliavimas
    - 5.2 Automatinė programų pažeidžiamumų paieška
    - 5.3 Konfigūracijų kontrolė
    - 5.4 Versijų ir pakeitimų kontrolė
    - 5.5 Testavimas saugioje aplinkoje (sandbox)

Saugos reikalavimai DK

6. **Virtualios infrastruktūros sauga**
    - 6.1 Hypervizorių sauga
    - 6.2 VM sauga
    - 6.3 Duomenų saugyklų sauga
    - 6.4 Diegimo ir valdymo sauga
    - 6.3 Virtualaus tinklo sauga
7. **Virtualaus tinklo sauga**
    - 7.1 Apsauga prieš tinklo lygio L3 atakas
    - 7.2 Konfigūracijų sauga
    - 7.3 Tinklo lygių segmentavimas
    - 7.4 Srauto šifravimas
    - 7.5 Virtualaus tinklo komponentų sauga

Saugos reikalavimai DK

8. **Gerosios praktikos**

- 8.1 Centralizuotų raktų, slaptažodžių valdymas
- 8.2 Įsilaužimo testavimai
- 8.3 Saugos auditavimas
- 8.4 Detalus informavimas
- 8.5 Saugos incidentų valdymas
- 8.6 Monitoringas ir žurnalai
- 8.7 Incidentų imitavimas ir reagavimo pratybos

Paslaugos tiekimo sutartis

Svarbus aspektas yra debesų **kompiuterijos paslaugos tiekimo sutartis** (SLO), kuri turi apibrėžti tiekimo objektą. Kartu turi būti sudaroma ir **paslaugos lygio tiekimo sutartis** (SLA), nustatanti ne tik charakteristikas, bet ir finansinės ir teisinės atsakomybės ribas.

Duomenų apsauga – svarbus SLA aspektas. Jis turi numatyti:

- Fizinę duomenų apsaugą, rezervinių kopijų darymą ir periodiškumą RPO, duomenų atstatymo laiką RTO.
- Apibrėžti duomenų turinio, kuris gali būti konfidencialus apsaugą ir galimas rizikas.

Informacijos sauga

Debesyse esančių duomenų, ypač asmens duomenų tvarkymas turi atitikti eilę ES ir LR teisės aktų:

1. Asmens duomenų teisinės apsaugos įstatymas
2. Valstybės informacinių išteklių valdymo įstatymas
3. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai
4. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai
5. ES direktyva 95/46/EB.