Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tadej Žarn

Primerjava zasebnega in javnega oblaka

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana, 2014

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Preučite bistvene značilnosti računalništva v oblaku, ki ga ločuje od drugih arhitekturnih oblik računalniških skupkov. Pojasnite različne namestitvene in storitvene modele in navedite primere. Kot osnovno tehnologijo, ki sploh omogoča velike oblačne infrastrukture, podrobneje preučite virtualizacijo. Pojasnite, kakšne vrste virtualizacije poznamo in kako jo upravljamo; komentirajte tudi vpliv virtualizacije na varnost in robustnost sistema kot celote. Pojasnite podobnosti in razlike med javnim in zasebnim oblakom tako na področju strukture kot tudi na področju organizacije in upravljanja. Navedite njune prednosti in slabosti z vidika podjetja, ki bi rado v oblak preneslo svoje ključne aplikacije ali podatke; pri ovrednotenju ne pozabite na varnostni vidik.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Tadej Žarn, z vpisno številko **63090305**, sem avtor diplomskega dela z naslovom:

Primerjava zasebnega in javnega oblaka

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 4. septembra 2014 Podpis avtorja:

Zahvaljujem se mentorici, doc. dr. Mojci Ciglarič, za usmerjanje in pomoč pri nastajanju diplomskega dela. Iskrena hvala mojim staršem in Termoelektrarni Brestanica, ker ste mi omogočili študij.

Kazalo

Slike

Seznam uporabljenih kratic

kratica	angleško	slovensko
ARP	address resoulution protocol	protokol za prepoznavanje naslovov
CMDB	configuration management database	sistem za upravljanje podatkovnih baz
CMS	content management system	sistem za upravljanje vsebin
CSA	cloud security alliance	neprofitna organizacija za promoviranje uporabe najboljših praks za zagotavljanje varnosti znotraj računalništva v oblaku
DDOS	distributed denial of service	porazdeljena zavrnitev storitve
GUI	graphical user interface	grafični uporabniški vmesnik
HIPPA	health insurance portability and accountability act	zakon o zdravstvenem zavarovanju in prenosu odgovornosti
IAAS	infrastructure as a service	infrastruktura kot storitev
IDS	intrusion detection system	sistem za zaznavanje vdorov
IGMP	internet group management protocol	protokol za upravljanje s skupinami
IP	internet protocol	internetni protokol
IT	information technology	informacijska tehnologija
LAN	local area networks	lokalno omrežje
MAC	media access control	nadzor nad dostopom večpredstavnosti
MPLS	multiprotocol label switching	večprotokolna komunikacija z zamenjavo label
NIC	network interface controller	omrežni vmesnik kartice

OSI model	open systems interconnection	predstavitev modularne zgradbe protokolov
PAAS	platform as a service	platforma kot storitev
PCI DSS	payment card industry data security standard	standard za varnost kartičnega poslovanja
RAID	redundant array of independent disks	standard za povezovanje dveh ali več trdih diskov
SAAS	software as a service	programska oprema kot storitev
SAN	storage area network	shranjevanje v omrežju
SLA	service-level agreements	sporazum o ravni storitve
SPAN	switched port analyzer	zrcaljenje vrat
SQL	structured query language	strukturiran povpraševalni jezik za delo s podatkovnimi bazami
TCO	total cost of operation	skupni stroški izvedbe
VDC	virtual device contexts	virtualna predstavitev naprave
VIP	virtual internet protocol	virtualni internetni protokol
VLAN	virtual local area network	virtualno lokalno omrežje
VM	virtual machine	virtualna naprava
VMM	virtual machine manager	upravitelj virtualne naprave
VN	virtual networks	virtualno omrežje
VRF	virtual routing and forwarding	virtualno usmerjanje in posredovanje
VSS	virtual switching system	virtualni sistem za preklapljanje
XSS	cross-site scripting	napad na spletno stran z vrinjenjem zlonamerne kode

Povzetek

Računalništvo v oblaku je model za zagotavljanje udobnega omrežnega dostopa na zahtevo do deljenega nabora računalniških virov. Bistvene značilnosti so samopostrežba na zahtevo, širok omrežni dostop, združevanje virov, hitra elastičnost in merjenje storitev. Med najbolj poznane in splošno uporabljene brezplačne storitve računalništva v oblaku sodijo družabna omrežja, spletne e-poštne storitve, spletne pisarne in dražbe. Pri računalništvu v oblaku poznamo štiri usmeritvene modele: zasebni, skupinski, javni in hibridni oblak. Pričujoče diplomsko delo obravnava primerjavo zasebnega in javnega oblaka, vrste virtualizacij ter upravljanje in nevarnosti pri virtualizaciji. Prikazana je vloga virtualnega stikala, kako deluje, kakšna je izolacija virtualnih naprav in kako se med seboj vidijo. V nalogi je bilo dokazano, da ima vsak oblak svoje prednosti in slabosti. Na podlagi zapisanega se uporabnik lažje odloči, na kateri oblak preiti.

Ključne besede: javni oblak, zasebni oblak, virtualizacija, hipervizor, virtualno stikalo.

Abstract

Cloud computing is a model for ensuring ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. The essential characteristics of cloud computing are on demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Some of generally more familiar cloud services are the e-mail web services, online offices and online auction websites. In cloud computing there are four deployment models: private, community, public and hybrid clouds. This paper compares private and public clouds. Furthermore, types of virtualisation are introduced along with virtualisation management and the risks of virtualisation. Moreover, the thesis depicts the role and the functioning of a virtual switch and outlines the isolation of virtual machines and their communication. The paper reveals that each cloud has its advantages and disadvantages, an overview of which makes the cloud decision process easier for the user.

Keywords: public cloud, private cloud, virtualization, hypervisor, virtual switch.

Poglavje 1

Uvod

Pri odločanju med zasebnim in javnim oblakom je treba dobro pretehtati, katere so prednosti in slabosti obeh. Zasebne oblake dandanes že dobro poznamo. Varnost imamo večinoma v svojih rokah. Poskrbeti moramo za vso infrastrukturo, izbrati ustrezno programsko opremo, virtualizacijske metode, stikala in ustrezno omrežno topologijo.

Ko preidemo na javni oblak, se stvari lahko zapletejo. Podatke, ki smo jih hranili na krajevnih računalnikih, sedaj prepuščamo ponudnikom javnih oblakov. V javnem oblaku strežnikov in ostale infrastrukture nimamo več tako pod nadzorom, kot smo jo imeli v zasebnem oblaku.

Obstaja kar nekaj prednosti javnega oblaka; ena izmed njih so nižji stroški. Druga prednost je ta, da lahko v javnem oblaku najamemo le, kar potrebujemo, in v primeru pomanjkanja pomnilniškega prostora, procesorske moči in kapacitete shranjevanja te tudi brez težav povečamo.

Izbiramo lahko med tremi storitvenimi modeli javnega oblaka, in sicer Programsko opremo kot storitev (SaaS), Platformo kot storitev (PaaS) in Infrastrukturo kot storitev (IaaS). Ti trije modeli so v nadaljevanju diplomskega dela podrobno opisani.

Po prebiranju diplomskega dela se bo uporabnik lažje odločil, na kateri oblak preiti. Predstavljene so nevarnosti, ki nam lahko pretijo tako v zasebnem, kakor tudi v javnem oblaku. Podrobno so opisane vrste virtualizacij, prednosti virtualizacij strežnika, povezave med zanesljivostjo in varnostjo v virtualizaciji, varnost virtualnih naprav – hipervizorjev, LAN stikal in delovanje virtualnih stikal.

Dandanes se ljudje pogosteje odločajo za javne oblake, vendar pa se mnogi ne zavedajo, kje vse se lahko znajdejo njihovi podatki. Pričujoče diplomsko delo naj bo uporabniku kot vodilo oz. priročnik za lažjo odločitev, kateri oblak izbrati.

Poglavje 2

Računalništvo v oblaku

Računalništvo v oblaku [1] je model za zagotavljanje vseprisotnega in udobnega omrežnega dostopa na zahtevo do dodeljenega nabora prilagodljivih računalniških virov (npr. do omrežja, strežnikov, pomnilniškega prostora, aplikacij in storitev), ki jih je mogoče z minimalnim vloženim trudom in interakcijo ponudnika storitev hitro pripraviti za uporabo in objaviti.

2.1 Bistvene značilnosti

Značilnosti računalništva v oblaku so naslednje: [1]

- **Samopostrežba na zahtevo.** Uporabnik lahko glede na trenutne potrebe samodejno in brez odvečne komunikacije s posameznimi ponudniki storitev ustvari računalniške zmogljivosti, kot sta strežniški čas in omrežni pomnilnik.
- **Širok omrežni dostop.** Zmogljivosti so na voljo prek omrežja in dostopne s pomočjo standardnih mehanizmov, ki podpirajo uporabo heterogenih tankih ali debelih platform (npr. mobilni telefoni, tablice, prenosniki in delovne postaje).
- **Združevanje virov.** Ponudnikovi računalniški viri so združeni, tako da lahko služijo več uporabnikom hkrati. Po načelu večodjemalskega modela so pri tem različni fizični in virtualni viri dinamično dodeljeni glede na zahteve

uporabnika. Pri tem podatki niso vezani na natančno lokacijo, tako da uporabnik običajno ne pozna natančne lokacije zagotovljenih virov oz. na lokacijo ne more vplivati, a lahko to določi na bolj abstraktni ravni (npr. lahko izbere državo, regijo ali podatkovne centre). Primeri virov vključujejo podatkovno shranjevanje, obdelavo, pomnjenje in omrežno pasovno širino.

- **Hitra elastičnost.** Zmogljivosti se lahko elastično ustvarijo ali sprostijo, v posameznih primerih samodejno, tako da se njihov obseg poveča in zmanjša sorazmerno s potrebo. Uporabnik zmogljivost razpoložljivih virov pogosto občuti kot neomejeno in jo lahko uporabi kadarkoli v kakršni koli količini.

- **Merjena storitev.** Sistemi v oblaku samodejno nadzirajo in optimizirajo uporabo virov z upravljanjem merilnih zmožnosti na določeni abstraktni ravni glede na vrsto storitve (npr. shranjevanje, obdelavo, pasovno širino in aktivne uporabniške račune). Uporabo virov je mogoče spremljati, nadzorovati in o njej poročati, kar zagotavlja transparentnost tako za ponudnika kot za uporabnika storitve. [1]

Tovrstna rešitev [2] poleg velike fleksibilnosti prinaša tudi potencialno nižje stroške poslovanja, saj uporabnikom omogoča, da plačajo le za dejansko porabljene kapacitete obdelave in shranjevanja podatkov.

V smislu fleksibilnosti storitev je najpomembneje, da uporabnik lahko najame storitve glede na trenutne potrebe, ki so lahko tudi povsem nepričakovane. Ko kapacitet ne potrebuje več, jih lahko preprosto sprosti. Ker vse to poteka dinamično, pri spremembi kapacitet strežnika ni treba ponovno zaganjati.

Računalništvo v oblaku zato predstavlja priložnost za mala in novonastala podjetja, saj ta v večini primerov nimajo lastne računalniške infrastrukture, potrebne za poslovanje, njena vzpostavitev pa lahko predstavlja prevelike stroške.

Ker se storitve ne poganjajo na krajevnih računalnikih, tudi ni potreb po zelo zmogljivi strojni opremi. Poganjati je treba le uporabniški vmesnik oblaka, ki je lahko kar spletni brskalnik ali pa deluje na podoben način.

Med najbolj poznane in splošno uporabljene brezplačne storitve računalništva v oblaku sodijo družabna omrežja, npr. Facebook in Twitter, spletne e-poštne storitve, denimo Gmail in Outlook, spletna mesta za deljenje slik (Flickr) in videov (YouTube, Netflix), spletne pisarne kot sta Google Docs in MS Office Online, sple-

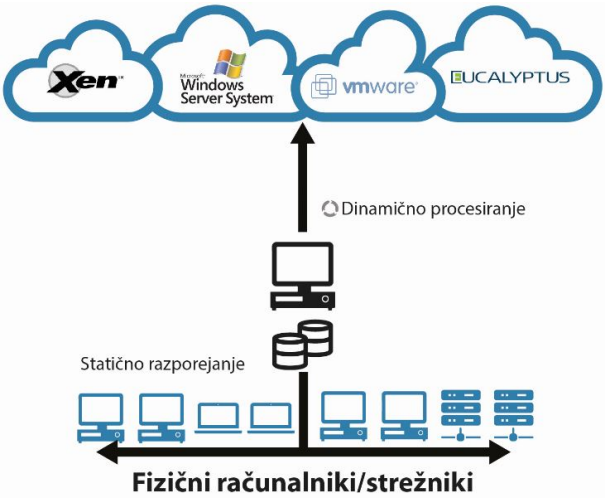
tne konference, npr. MS Office Live Meeting, spletne dražbe, recimo eBay itn.[2]

2.2 Vrste računalništva v oblaku

Pri računalništvu v oblaku [3] poznamo štiri usmeritvene modele, ki so prikazani na sliki 2.1:

Slika 2.1: Prikaz zasebnega, javnega in hibridnega oblaka. [3]

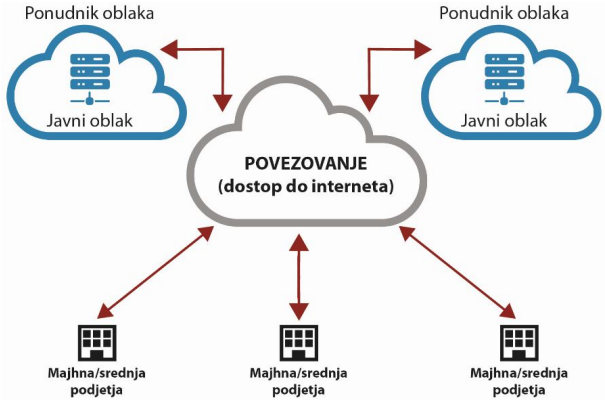
- **Zasebni oblak.** Infrastruktura oblaka [1, 4] je namenjena samo za uporabo ene organizacije, ki si želi imeti svoj oblak in ima več uporabnikov (npr. poslovnih enot). S oblakom lahko upravlja, ga nadzoruje oz. si ga lasti organizacija, tretja oseba ali kombinacija teh. Lahko je nameščen na uporabnikovi lokaciji oz. izven nje. S zasebnim oblakom je mogoče izkoristiti številne prednosti javnega računalništva v oblaku, vključno s samopostrežbo storitev, razširljivostjo in elastičnostjo, hkrati pa zagotoviti dodaten nadzor in možnosti prilagajanja.



Slika 2.2: Zasebni oblak.

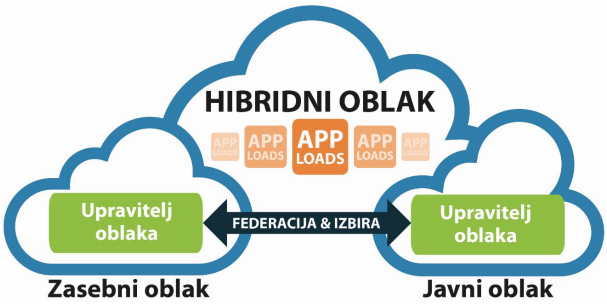
- **Skupinski oblak.** Infrastruktura oblaka je namenjena [1] samo za uporabo specifične skupnosti uporabnikov iz organizacij, ki imajo skupne interese (npr. skupno nalogo, varnostne zahteve, pravila in skladnostne zahteve). Z oblakom lahko upravlja, ga nadzoruje oz. si ga lasti ena ali več organizacij v skupnosti, tretja oseba ali kombinacija teh. Lahko je nameščen na uporabnikovi lokaciji oz. izven nje.

- **Javni oblak.** Infrastruktura oblaka je na voljo splošni javnosti [1, 5] za prosto uporabo. Z oblakom lahko upravlja, ga nadzoruje oz. si ga lasti podjetje, akademska ali vladna organizacija ali kombinacija teh. Nameščen je na lokaciji ponudnika oblaka. Tukaj morajo ponudniki upoštevati visoko učinkovitost, varnost in lokalnost podatkov. Prednost javnega oblaka je njegova velikost in tako posledično tudi večja skalabilnost in varnost. Dele javnega oblaka uporabimo izključno za enega odjemalca in tako pridobimo zasebni virtualni center. S tem pridobimo boljši vpogled v infrastrukturo in nadzor nad strežnikom in sistemom shranjevanja.



Slika 2.3: Javni oblak.

- **Hibridni oblak.** Infrastruktura oblaka je sestavljena iz enega ali več različnih oblakov (zasebnega, skupinskega in javnega) [1, 6], ki pa ostanejo ločene enote, le da so povezane s pomočjo standardizirane ali lastniške tehnologije, ki omogoča prenos podatkov in aplikacij (npr. razširitev oblaka za izenačevanje obremenitev med oblaki). Tovrstne oblake uporabljamo za poslovne zadeve zaradi visokega nivoja ščitenja podatkov in velike računalniške moči. Problemi v tem modelu nastanejo, ko moramo odločati med količino podatkov in procesno močjo, ki vpliva na učinkovitost oblaka.



Slika 2.4: Hibridni oblak. [6]

2.3 Storitveni modeli

Programska oprema kot storitev (SaaS). Uporabniku je omogočen dostop do uporabe aplikacij ponudnika, ki so že bile postavljene na infrastrukturo ponudni-

kovega oblaka. Pod infrastrukturo oblaka uvrščamo zbirko strojne in programske opreme. Infrastrukturo oblaka lahko dojemamo kot celoto, ki vključuje fizično in abstraktno raven. Fizična raven vključuje strojne vire, ki jih potrebujemo za podporo ponujene storitve oblaka, in običajno vsebuje strežnik, pomnilnik in omrežne komponente. Abstraktna raven je sestavljena iz programov, ki so nameščeni prek fizične ravni, in predstavljajo osnovne značilnosti oblaka. Aplikacije so dostopne z različnih uporabniških naprav prek tankih vmesnikov, kot npr. spletnih iskalnikov (npr. spletni poštni odjemalci) ali programskih vmesnikov. Uporabnik nima nadzora nad osnovno infrastrukturo, oblaka vključno z omrežjem, s strežniki, z operacijskimi sistemi, s pomnilnikom oz. celo s posameznimi zmogljivostmi aplikacije, z morebitno izjemo omejenih nastavitev aplikacije, ki so specifične za uporabnika. [1]

Platforma kot storitev (PaaS). Ponudnik dovoljuje uporabniku, da na infrastrukturo oblaka naloži svoje aplikacije s pomočjo programskih jezikov, knjižnic, storitev in orodij, ki jih podpira ponudnik. Uporaba kompatibilnega programskega jezika, knjižnic, storitev in orodij iz drugih virov načeloma ni popolnoma onemogočena. Uporabnik nima nadzora nad osnovno infrastrukturo oblaka, vključno z omrežjem, s strežniki, z operacijskimi sistemi, s pomnilnikom; lahko pa nadzira postavljene aplikacije in v nekaterih primerih konfiguracijske nastavitve za gostujoče aplikacijsko okolje. [1]

Infrastruktura kot storitev (IaaS). Ponudnik uporabniku zagotavlja obdelavo, pomnilnik, omrežja in druge temeljne računalniške vire, pri čemer lahko uporabnik naloži in zažene poljubno programsko opremo, vključno z operacijskimi sistemi in aplikacijami. Uporabnik ne upravlja ali nadzira osnovne infrastrukture oblaka, ima pa nadzor nad operacijskimi sistemi, pomnilnikom in postavljenimi aplikacijami. V nekaterih primerih ima tudi omejen nadzor nad izbranimi komponentami omrežja (npr. požarni zid). [1]

Slika 2.5: Storitveni modeli in glavni ponudniki. [7]

Poglavje 3

Virtualizacija

Virtualizacija je programska tehnologija, ki omogoča deljenje fizičnih virov (npr. strežnika) in jih razdeli na več virtualnih naprav (ang. *virtual machines*). [18]

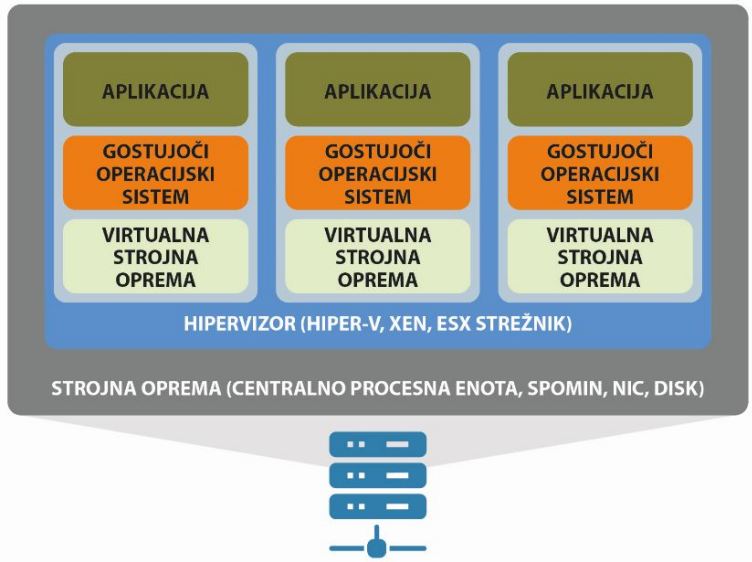
Virtualizacija računalniškega sistema med dve abstraktni plasti v sistemu doda še eno. Abstraktna raven je programska plast med strojno opremo in gostujočimi operacijskimi sistemi. Plast deluje kot upravljalnik virov, tako da omogoča skupno rabo procesorskih moči in pomnilnikov. Ta programska oprema se imenuje nadzornik virtualnih naprav (ang. *virtual machine monitor* - VMM) oz. hipervizor. Virtualizacija strežnika spremeni vsa pravila, saj razbije tradicionalni model fizičnega strežnika v vlogi gostitelja enega samega operacijskega sistema na več virtualnih naprav na enem samem strežniku. To pa stori z uporabo hipervizorja. Tako ima hipervizor nadzor nad vsemi virtualnimi napravami. Več operacijskih sistemov (OS) lahko ločeno sobiva na isti virtualni napravi in sočasno deluje na enem strežniku. [18]

Takšna oblika virtualizacije dopušča, da podatkovni centri povečajo svojo uporabo virov. Za boljši izkoristek strežnika so virtualni viri, na katerih gostujejo posamezne aplikacije, povezani s fizičnimi viri. To še posebej velja za računalništvo v oblaku - več fizičnih virov je zbranih v en sam oblak. Razlika med virtualizacijo in oblakom je, da je virtualizacija sredstvo, ki omogoča vzpostavitev in upravljanje oblakov. Virtualizacija se v tem primeru nanaša na virtualizacijo operacijskih sistemov, ki jo podpirajo npr. VMware, Xen in ostale tehnologije, zasnovane na hipervizorju. [7, 18]

Glavne prednosti virtualizacije:

- dostop do strežnika, omrežja in virov shranjevanja na zahtevo,
- varčevanje z energijo za zeleno zemljo,
- fizično zmanjšanje prostora,
- zmanjšanje stroškov iskanja osebja, ki ga je težko najti,
- zmanjšanje kapitala in stroškov izvedbe.

Pri računalništvu v oblaku poznamo različne zvrsti virtualizacije, kot so omrežje, računalniki, shranjevanje in storitve. [7]



Slika 3.1: Virtualizacija strežniškega okolja. [9]

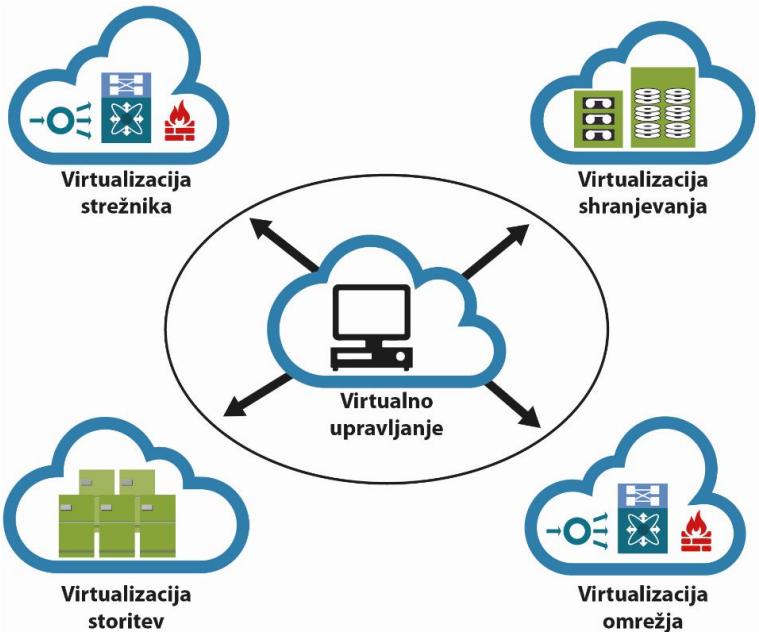
3.1 Vrste virtualizacij

Poznamo več vrst virtualizacij: [7]

- virtualizacija strežnika,
- virtualizacija shranjevanja,

- virtualizacija omrežja in
- virtualizacija storitve.

Slika 3.2 prikazuje virtualizacijo strežnika, virtualizacijo omrežja, virtualizacijo shranjevanja in virtualizacijo storitve, ki se nahajajo v podatkovnem centru.

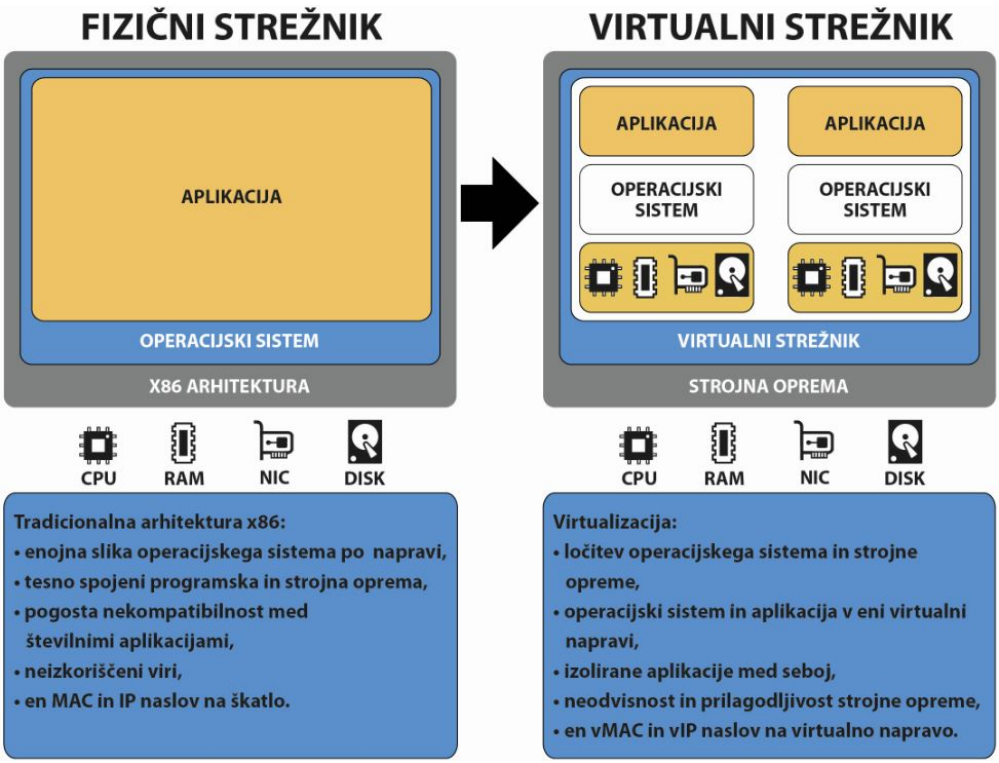


Slika 3.2: Vrste virtualizacij. [7]

3.1.1 Virtualizacija strežnika

Virtualizacija strežnika (tudi virtualizacija strojne opreme) [7] je dandanes najbolj znana aplikacija za virtualizacijo strojne opreme. Današnja x86 računalniška strojna oprema je bila oblikovana za izvajanje enega operacijskega sistema in ene aplikacije. Tako je veliko naprav v večji meri ostalo neizkoriščenih. Virtualizacija omogoča poganjanje več virtualnih naprav na eni fizični napravi. Virtualne naprave si delijo vire fizičnega računalnika v več različnih okoljih. Različne virtualne naprave lahko poganjajo različne operacijske sisteme in različne aplikacije na enem fizičnem računalniku.

Slika 3.3 prikazuje virtualni strežnik v primerjavi s fizičnim strežnikom brez virtualizacije. Programska oprema hipervizorja omogoča ustvarjanje virtualne naprave (ang. *virtual machine*), ki posnema fizični računalnik z ustvarjanjem ločenega okolja operacijskega sistema, ki je logično ločeno od strežniškega gostitelja. Hipervizor ali nadzornik virtualne naprave (ang. *virtual machine manager* – VMM) je program, ki dopušča, da si različni operacijski sistemi delijo enega strežniškega gostitelja. Ena sama fizična naprava se lahko uporabi za nastajanje več virtualnih naprav, ki lahko neodvisno in istočasno poganjajo več operacijskih sistemov. Virtualne naprave so shranjene kot datoteke, kar omogoča enostavno ponovno vzpostavitev sistema, ki je odpovedal – kot da bi kopirali datoteke na novo napravo. [7]



Slika 3.3: Virtualizacija strežnika. [7]

Prednosti virtualizacije strežnika

Obstaja kar nekaj prednosti virtualizacije strežnika: [7]

- **Particioniranje (delitev na particije).** Omogoča zagon več operacijskih sistemov. Omogoča razdelitev fizičnih sistemskih virov med virtualne naprave. Virtualne naprave se ne zavedajo obstoja drugih virtualnih naprav.
- **Upravljanje.** Okvara ene virtualne naprave ne vpliva na ostale virtualne naprave. Upravljalni procesi se lahko zaženejo ločeno na vseh virtualnih napravah, tako da se ugotovi zmogljivost posamezne virtualne naprave in aplikacij, ki se na njih izvajajo.
- **Inkapsulacija.** Celotno stanje virtualne naprave je mogoče shraniti v eni datoteki. Premikanje in kopiranje podatkov virtualne naprave je enostavno (kot kopiranje datotek).
- **Prilagodljivost.** Dovoljuje oskrbo in migracijo katerekoli virtualne naprave k podobni napravi na kateremkoli fizičnem strežniku. Uporaba več operacijskih sistemov, na primer Windowsa in Linuxa, omogoča spremembe konfiguracije virtualne naprave, ne da bi se ta zrušila.

Virtualizacija strežnika je ključna gonilna sila za zmanjšanje števila fizičnih strežnikov in fizičnega prostora, hlajenja, uporabe kablov in stroškov kapitala v vseh projektih združitve podatkovnih centrov. [7]

3.1.2 Virtualizacija shranjevanja

Virtualizacija shranjevanja [7] omogoča logični abstraktni pogled na fizične naprave za shranjevanje. Virtualizacija shranjevanja omogoča več uporabnikom ali aplikacijam dostop do prostora za shranjevanje, ne da bi jih skrbelo, kje se ta prostor fizično nahaja in kako ga upravljati. Omogoča fizično shranjevanje v okolju, ki ga uporablja več aplikacijskih strežnikov in fizičnih naprav za virtualizacijskim slojem, ki se jih dojema in upravlja kot ogromen prostor za shranjevanje brez fizičnih meja. Virtualizacija shranjevanja prikriva dejstvo, da v neki organizaciji obstajajo ločene naprave za shranjevanje, saj ustvari vtis, da vse naprave delujejo kot ena sama naprava. Virtualizacija skrije zapleten proces shranjevanja samih podatkov

in ponovnega prikaza, ko so ti potrebni. Navadno se virtualizacija shranjevanja nanaša na zbirko večjih shramb omrežja za shranjevanje podatkov (ang. *Storage Area Network* – SAN), a se prav tako uporablja za logično particioniranje strojne opreme lokalnega namizja in redundantnega diskovnega polja (ang. *Redundant Array of Independent Disks* – RAID). Večja podjetja že dalj časa izkoriščajo prednosti tehnologij omrežja za shranjevanje podatkov, pri katerih shramba ni več povezana s serverji, ampak neposredno z omrežjem. Z deljenjem podatkov na omrežju omrežja za shranjevanje podatkov omogočajo nadgradljivo in prilagodljivo razporeditev virov shranjevanja, učinkovito rešitev varnostnih kopij in večjo uporabo shrambe. [7]

Prednosti virtualizacije shranjevanja

Prednosti virtualizacije shranjevanja so naslednje: [7]

- **Optimizacija virov.** Tradicionalno je naprava za shranjevanje fizično povezana in dodeljena strežnikom in aplikacijam. Če potrebujemo večjo kapaciteto, kupimo več trdih diskov, ki se dodajo strežniku in dodelijo aplikacijam. Posledica tega načina delovanja je, da ostane velik del shrambe neizkoriščen. Virtualizacija shranjevanja omogoča prostor za shranjevanje po potrebi brez izgub, podjetjem pa ponuja možnost, da bolj učinkovito uporabijo že obstoječe komponente za shranjevanje, ne da bi morali dokupiti nove.

- **Stroški delovanja.** Dodajanje neodvisnih virov hrambe in konfiguriranje posameznih strežnikov in aplikacij je zamudno in zahteva visoko usposobljeno delovno silo, ki pa jo je težko najti, kar posedično vpliva na celotne stroške lastništva (ang. *Total Cost of Ownership* – TCO). Virtualizacija shranjevanja omogoča dodajanje virov hrambe brez upoštevanja aplikacije. Vire shranjevanja se lahko doda v prostor za shranjevanje z metodo "vleci in spusti" s pomočjo upravljalne konzole. Varna upravljalna konzola z grafičnim uporabniškim vmesnikom (ang. *Graphical User Interface* – GUI) poveča varnost in operacijskim osebam omogoči enostavno dodajanje virov shranjevanja.

- **Večja razpoložljivost.** Pri tradicionalnih shranjevalnih aplikacijah lahko predviden čas izpada za vzdrževanje in posodabljanje programske opreme

ter nepredviden čas izpada zaradi virusov in izpadov elektrike za uporabnike pomeni prekinitev delovanja aplikacije. Posledica tega je nezmožnost upoštevanja dogovorov o ravni storitve (ang. *Service-Level Agreements* – SLA), kar lahko povzroči nezadovoljstvo in izgubo strank. Virtualizacija shranjevanja zagotovi nove vire shranjevanja v najkrajšem možnem času ter izboljša vsesplošno dostopnost virov.

- **Izboljšana zmogljivost.** V kolikor več sistemov izvaja eno opravilo, lahko le-to en sistem shranjevanja preobremeni. Če se z virtualizacijo delovna obremenitev porazdeli na več naprav za shranjevanje, se zmogljivost poveča. Poleg tega je mogoče vgraditi tudi nadzor varnosti v shrambah, tako da je dostop do podatkov dovoljen le pooblaščenim aplikacijam ali strežnikom. [7]

3.1.3 Virtualizacija omrežja

Virtualizacija omrežja je med vsemi virtualizacijami verjetno najbolj neopredeljiva. Obstaja več vrst virtualizacij omrežja: [7]

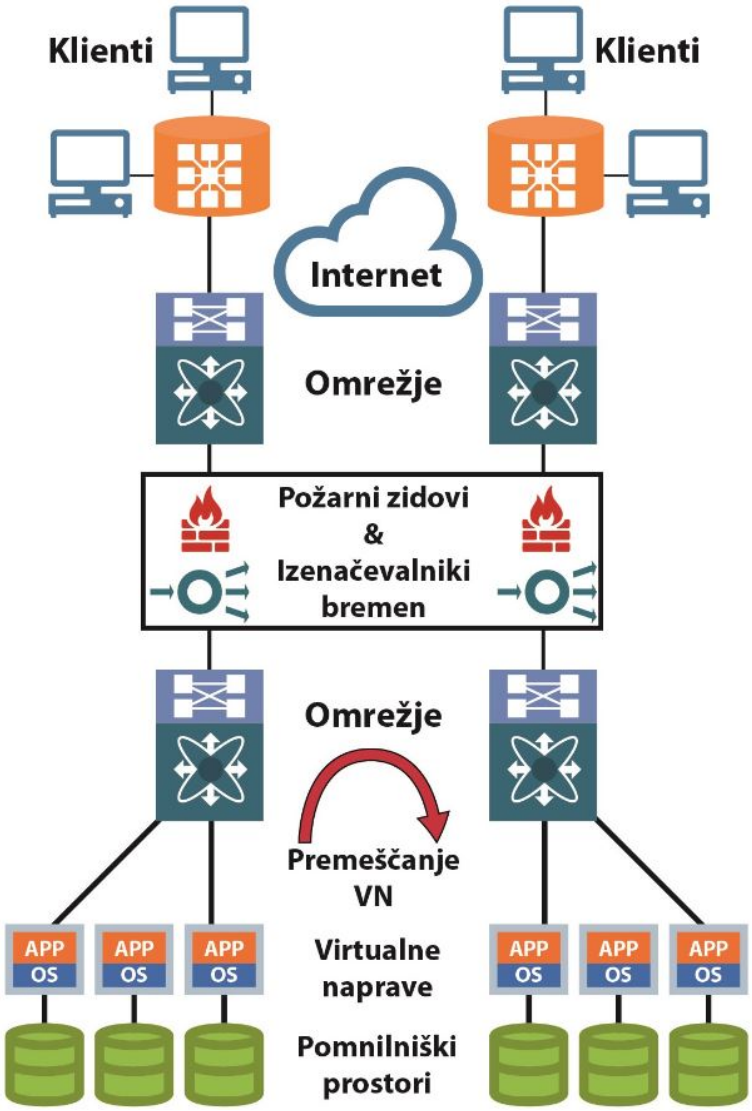
- VLAN je preprost primer virtualizacije omrežja. VLANi dovoljujejo logično segmentacijo LANa v več razpršitvenih domen. VLANi so definirani na stikalu na osnovi vrat. Torej se lahko odločite, da bodo vhodi 1–10 del VLANa 1 in vhodi 11–20 del VLANa 2. Ni treba, da so vhodi v istem VLANu drug ob drugem. Ker gre za logično in ne fizično segmentacijo, ni potrebno, da se delovne postaje, ki so povezane z vhodi, nahajajo v neposredni bližini. Uporabniki, ki so povezani v LAN, se lahko nahajajo v različnih nadstropjih ali v različnih stavbah.

- Virtualno usmerjanje in posredovanje (ang. *Virtual Routing and Forwarding* – VRF), ki se pogosto uporablja v omrežjih večprotokolne komutacije z zamenjavo label (ang. *Multi-Protocol Label Switching* – MPLS), omogoča več primerov sočasnega obstoja usmerjevalne tabele znotraj istega usmerjevalnika. S segmentacijo omrežnih poti brez uporabe več naprav se tako poveča funkcionalnost. Ker se promet samodejno izolira, VRF poveča omrežno varnost in odstrani potrebo po šifriranju in avtentikaciji.

- VDC (ang. *Virtual Device Contexts*) je koncept virtualizacije podatkovnega centra, ki se uporablja za virtualizacijo naprave, ki predstavlja fizično stikalo kot številne logične naprave. VDC lahko vsebuje svojo lastno in neodvisno množico VLANov in VRFjev. Vsak VDC ima lahko dodeljena fizična vrata, kar omogoča tudi virtualizacijo ravni podatkov strojne opreme. V vsakem VDCju se ustvari ločena upravljalna domena, ki upravlja VDC in s tem dopušča tudi virtualizacijo ravni upravljanja. Vsak VDC je za povezane uporabnike na videz edinstvena naprava.

- Virtualna omrežja (ang. *Virtual Networks* – VN) predstavljajo računalniška omrežja, ki so vsaj delno sestavljena iz virtualnih omrežnih povezav. Takšna povezava ni sestavljena iz fizične povezave med dvema viroma, ampak se izvede z metodami virtualizacije omrežja. Tehnologije virtualnih omrežnih povezav so razvite kot most med strežnikom, shrambo in omrežjem upravljalne domene, ki omogoča, da se podatki o spremembah v enem okolju posredujejo drugim. Ko uporabnik, na primer v okolju VMware vSphere, uporabi vCenter za zagon VMotion, da premakne virtualno napravo z enega fizičnega strežnika na drugega, se ta dogodek sporoči podatkovnemu centru in omrežju za shranjevanje podatkov (SAN). Ustrezni omrežni profil in storitve shranjevanja se premaknejo skupaj z virtualno napravo. [7]

Slika 3.4 ponazarja medsebojno delovanje virtualiziranega omrežja, računalnika in shranjevanja v infrastrukturi.



Slika 3.4: Virtualizacija omrežja. [7]

Ko je pravilno oblikovana, je virtualizacija omrežja v širšem smislu podobna virtualizaciji strežnika, in sicer v tem, da je skupna fizična infrastruktura omrežja varno deljena med skupinami uporabnikov, aplikacij in naprav. [7]

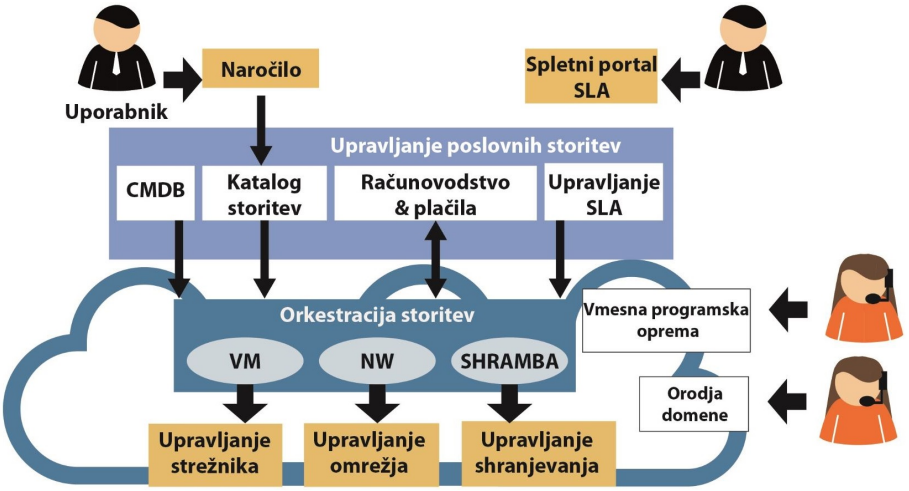
3.1.4 Virtualizacija storitve

Virtualizacija storitve [7] v podatkovnih centrih se nanaša na storitve, kot je storitev požarnega zidu za dodatno varnost ali na storitev izenačevanja obremenitve za dodatno zmogljivost in zanesljivost. Virtualni vmesnik, ki ga pogosto imenujemo virtualni internetni protokol (VIP), je izpostavljen zunanjemu svetu in se predstavlja kot dejanski spletni strežnik. Ta upravlja povezave do in od spletnega strežnika, ko je to potrebno. To omogoči izenačevalcu obremenitev, da enkratno upravlja z več spletnimi strežniki ali aplikacijami, kar zagotavlja bolj varno in robustno topologijo kot v primeru, ko je uporabnikom dovoljen neposredni dostop do posameznih spletnih strežnikov. Gre za predstavitev virtualizacije tipa "ena proti mnogo". Na zunaj izgleda, kot da je strežnik le eden, a ta za povratno proxy napravo skriva več strežnikov. [7]

3.2 Upravljanje virtualizacije

Upravljanje virtualizacije [7] se nanaša na zagotavljanje in organizacijo virtualnih virov kot tudi na čas izvajanja usklajevanja razpoložljivih virov in virtualnih instanc. Ta funkcija vključuje statično in dinamično preslikavo virtualnih virov na fizične vire ter vsesplošne vidike upravljanja, kot so zmogljivost, analitika, plačevanje in SLA (ang. *service-level agreements*).

Na sliki 3.5 je prikazana interakcija med omrežjem, računalnikom in pomnilnikom na upravljalni/organizacijski ravni, kar omogoča dostop do storitev v skoraj realnem času. Storitve se običajno prestavijo na raven portala uporabnika, kjer uporabnik izbere storitev in se ta zagotovi s pomočjo različnih domen in upravljalnih sistemov vmesne opreme, vključno s konfiguracijsko podatkovno bazo (ang. *configuration management database* - CMDB), s storitvenim katalogom, z obračunom ter s sistemom povrnjenih stroškov (ang. *chargeback*), s SLA upravljanjem, z upravljanjem storitev in s portalom storitev.



Slika 3.5: Upravljanje virtualizacije. [7]

Virtualizacija omrežja, računalnika in pomnilnika odločilno vpliva na IT [7], tako da omogoča prilagodljive in na napake odporne storitve, ki so ločene od fiksnih tehnoloških komponent. Tako ni več treba vzdrževati orodij za nadziranje strojne opreme in nepovezanih aplikacij ter posodabljati osnovne strojne opreme. Strojno opremo je mogoče popraviti ali nadgraditi, aplikacije pa vrniti nazaj na izboljšano infrastrukturo brez vzdrževalnega orodja. Druge prednosti virtualizacije so še: učinkovita uporaba neizkoriščenih virov, zmanjšanje upravljanih sredstev strojne opreme in zmanjšanje števila pogodb o vzdrževanju strojne opreme. Čeprav virtualizacija prinaša veliko prilagodljivost, po drugi strani poveča potrebo po nadzoru in upravljanju storitev za zagotovitev večje situacijske ozaveščenosti. V preteklosti je lahko administrator z gotovostjo rekel: "Moja podatkovna baza deluje na strežniku X, ki je povezan s stikalom B in uporablja pomnilniško polje C." Virtualizacija to povezavo prekine in omogoča, da se ti infrastrukturni viri uporabijo na način, ki podpira več nadgraditev in je bolj učinkovit. Aplikacija je lahko nameščena na katerem koli računalniškem vozlišču v skupini strežnikov, lahko uporablja pomnilniški prostor na kateri koli pomnilniški napravi, lahko uporablja virtualno omrežje in se lahko, da zadosti zmogljivostim in operacijskim potrebam, prestavi. Razumevanje medsebojnih povezav pred samim vzdrževanjem je tako še bolj pomembno. [7]

Razlika med virtualizacijo in računalništvom v oblaku je ta, da je virtuali-

zacija tehnologija. Hipervizor predstavlja srce in dušo strežniške virtualizacije, računalništvo v oblaku pa vključuje virtualizacijo. Pri oblaku ni plasti, ki bi bila podobna ravni hipervizorja, skozi katerega gredo podatki. Pri oblaku bo sicer najverjetneje potrebna virtualizacija strežnika, a to še ni dovolj za delovanje oblaka. V oblaku so vključeni viri predstavljeni tako, da uporabniku zagotavljajo izvajanje storitev na zahtevo po meri in v večnajemniškem okolju. Računalništvo v oblaku se večinoma poslužuje enake infrastrukture, orodij za upravljanje storitev, orodij za upravljanje virov, organizacijskih sistemov, CMS/CMDBjev, strežniške platforme, omrežnnih povezav, pomnilniškega polja itd. Uporabniku se ponavadi zagotovi samopostrežni portal, na katerem lahko naroči storitev in skrije vso fizično kompleksnost infrastrukture in upravljanja. [7]

3.3 Povezava med zanesljivostjo in varnostjo v virtualizaciji

Pri virtualizaciji na zmogljivost oblaka poleg varnosti vplivajo tudi vprašanja, povezana z zanesljivostjo. Ponudnik lahko na primer na fizičnem strežniku združi preveč virtualnih naprav. Posledica so težave z zmogljivostjo, ki jih povzročijo omejeni CPE cikli ali vhodne/izhodne motnje. Te težave se lahko pojavijo na navadnem fizičnem strežniku, vendar so pogostejše pri virtualnih strežnikih (zaradi povezav fizičnega strežnika z več virtualnimi napravami, pri čemer se vsi potegujejo za kritične vire). Opravila upravljanja, kot npr. upravljanje delovanja in upravljanje načrtovanja procesorske moči, so bolj kritična v virtualnem okolju kot v fizičnem okolju. To pomeni, da mora biti organizacija informacijske tehnologije sposobna nadzorovati uporabo tako fizičnih strežnikov kot virtualnih naprav v realnem času. Ta zmogljivost organizaciji informacijske tehnologije omogoča, da prepreči preveliko oz. premajhno uporabo virov strežnika, kot npr. CPE in spomin, ter dodeli vire glede na spreminjajoče se uporabniške zahteve. [10]

Organizacije, ki ponujajo oblake, so pri virtualizaciji soočene tudi z izzivom, kako upravljati širitev virtualnih naprav. Problematika pri širitvi virtualnih naprav je preobremenjenost infrastrukture. Za preprečitev širitve virtualnih naprav morajo upravljavci virtualnih naprav natančno analizirati potrebe vseh novih vir-

tualnih naprav in nepotrebne virtualne naprave prenesti na druge fizične strežnike. Poleg omenjenega se lahko nepotrebna virtualna naprava prenese z enega fizičnega strežnika na drugega z visoko razpoložljivostjo in energetsko učinkovitostjo. Vsekakor je treba upoštevati, da ohranimo varnost virtualnih naprav, ki jih prenesemo. Treba je zagotoviti varnost na novi lokaciji in ohraniti nastavitve prenesenih virtualnih naprav. [10]

3.3.1 Varnost virtualnih naprav

Virtualizacija ni tako nova tehnologija kot oblak, a zajema več varnostnih vprašanj, ki so se prenesla na tehnologijo oblaka. Obstajaja nekaj slabosti virtualizacij in pojavljajo se vprašanja o varnosti, ki so značilna za okolje oblaka. [10]

Varnost hipervizorja

V virtualnem okolju obstaja več virtualnih naprav, ki lahko imajo samostojne varnostne cone, do katerih druge virtualne naprave, ki imajo svoje cone, ne morejo dostopati. Hipervizor ima svojo lastno varnostno cono in je kontrolni agent za vse znotraj virtualnega gostitelja. Hipervizor se lahko dotika in vpliva na vse operacije virtualnih naprav, ki delujejo znotraj virtualnega gostitelja. Obstaja več varnostnih con, a te varnostne cone se nahajajo znotraj ene fizične infrastrukture. To lahko ogrozi varnost, ko napadalec prevzame nadzor nad hipervizorjem. Napadalec ima tako popolni nadzor nad vsemi podatki znotraj območja hipervizorja. Drugi bistveni varnostni pomislek pri virtualizaciji je “pobeg iz virtualne naprave” ali možnost dostopa do hipervizorja z notranje ravni virtualne naprave. To povzroči težave, saj se za virtualne platforme ustvari vedno več programskih vmesnikov. Skupaj s programskimi vmesniki se ustvarijo tudi nadzori za deaktivacijo funkcionalnosti znotraj virtualne naprave, kar lahko zmanjša zmogljivost in dosegljivost. [10]

Prednosti in slabosti sistemov s hipervizorjem

Hipervizor ima poleg sposobnosti upravljanja virov tudi potencial za varovanje infrastrukture oblaka. [10]

Prednosti sistemov s hipervizorjem:

- Hipervizor nadzira strojno opremo in je tudi edini, ki lahko do nje dostopa. To virtualni tehnologiji, ki temelji na hipervizorju, omogoča varno infrastrukturo. Hipervizor lahko deluje kot požarni zid in lahko prepreči zlonamernim uporabnikom, da bi ogrozili strojno infrastrukturo.
- Hipervizor se vgradi v gostujoči operacijski sistem v računalniški hierarhiji oblaka, kar pomeni, da lahko v primeru napada na varnostni sistem v gostujočem operacijskem sistemu hipervizor tega tudi zazna.
- Hipervizor se uporablja kot abstraktna raven za izolacijo virtualnega okolja od strojne opreme, na katero je nameščen.
- Pri virtualizaciji hipervizor na svoji ravni nadzoruje vsak dostop med gostujočimi operacijskimi sistemi in skupno strojno opremo. Hipervizor lahko tako poenostavi proces prenosa in nadzora v okolju oblaka.

Nekaj slabosti, ki lahko vplivajo na storilnost uporabljenih varnostnih metod:

- Pri virtualizaciji, ki temelji na hipervizorju, je samo en hipervizor, sistem pa postane kritična točka odpovedi. Če se hipervizor zaradi preobremenitev ali uspešnega napada sesuje, bodo prizadeti vsi sistemi in virtualne naprave.
- Podobno kot druge tehnologije je hipervizor dovzeten za nekatere napade, kot na primer prekoračitev medpomnilnika.

Upravljanje varnosti pri virtualizaciji, ki temelji na hipervizorju

Kot je že bilo omenjeno, hipervizor deluje kot orodje za upravljanje. Glavni namen cone hipervizorja je vzpostavitev cone zaupanja okoli strojne opreme in navideznih naprav. Druge navidezne naprave, ki so na voljo, so na preizkušnji hipervizorja, na katerega se lahko zanesejo, saj uporabniki pričakujejo, da bodo administratorji naredili vse, da bodo zagotovili varnost. [10]

Pri upravljanju varnosti s hipervizorjem obstajajo tri glavne ravni:

- **Avtentikacija.** Uporabniki se morajo pri prijavi v svoj račun pravilno avtenticirati, tako da uporabijo primerne in standardne mehanizme, ki so na voljo.
- **Avtorizacija.** Uporabniki morajo imeti dovoljenje za dostop do želenih podatkov ali aplikacij.
- **Omreženje.** Omrežje mora biti zasnovano z mehanizmi, ki zagotavljajo varne povezave med samimi aplikacijami, ki so najverjetneje nameščene na drugi varnostni coni kot navaden uporabnik.

Avtentikacija in avtorizacija sta najbolj nujna nadzorna vidika upravljanja, saj je za namen nadzora virtualnega gostitelja na voljo več različnih metod. Splošno prepričanje je, da je povezava pri prenosih med uporabniki in hipervizorjem najbolj pomembna zadeva, a za varnost pri virtualizaciji je poleg same povezave pomembno še veliko več. Enako pomembno je na primer razumevanje programskih vmesnikov in osnovnih konceptov razpoložljivega hipervizorja in virtualnih naprav ter delovanje varnostnih orodij za upravljanje. Če se lahko varnostni upravitelj posveti tako avtentikaciji, avtorizaciji, virtualni strojni opremi in varnosti hipervizorja, kot tudi varnosti omrežja, so uporabniki oblaka na dobri poti do celostne varnostne politike. Če se ponudnik oblaka za izvedbo teh opravil na ravni virtualizacije zanaša samo na varnost omrežja, bo implementirano virtualno okolje izpostavljeno tveganju. Ponudnik oblaka mora tako poskrbeti za vzpostavitev močnega in varnega omrežja, kot tudi za komunikacijo med virtualno napravo in hipervizorjem. [10]

3.3.2 Nevarnosti in napadi pri virtualizaciji

Nevarnosti

Pri upravljanju hipervizorja [10] vidijo vsi uporabniki svoj sistem kot samostojen računalnik, ki je izoliran od ostalih uporabnikov, čeprav vse uporabnike oskrbuje ista naprava. V tem smislu je virtualna naprava operacijski sistem, ki ga upravlja prikrit nadzorni program.

Poznamo naslednje nevarnosti in napade pri virtualizaciji:

- **Napadi na ravni virtualne naprave.** Potencialna slabost je tehnologija hipervizorja oz. virtualne naprave, ki jo ponudniki oblaka uporabljajo v večuporabniški arhitekturi. Te tehnologije vključujejo "virtualne naprave", oddaljene verzije tradicionalnih računalniških sistemov na lokaciji uporabnika, vključno s strojno opremo in z operacijskim sistemom. Število teh virtualnih naprav se lahko skladno s potrebami hitro poveča oz. zmanjša, kar pomeni večjo učinkovitost.

- **Slabosti ponudnika oblaka.** Te so lahko na ravni platforme, še bolj pa na ravni aplikacije, kot na primer SQL-vrinjenje ali dovzetnost za XSS-napad na ravni storitve oblaka, in posledično zmanjšajo varnost okolja.

- **Avtentikacija in avtorizacija.** Avtentikacijski in avtorizacijski okvir se v oblak ne razširi samodejno. Podjetja morajo združiti varnostno politiko oblaka s svojo lastno varnostno politiko.

- **Odvisnost.** Računalništvo v oblaku je velikokrat odvisno od ponudnika. V primeru, da ponudnik oblaka propade, mora uporabnik sam poskrbeti za shranjevanje podatkov.

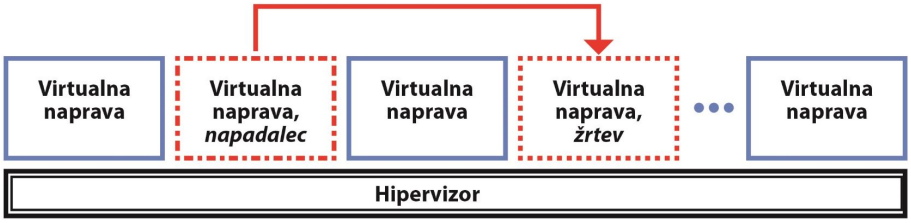
- **Nadzor podatkov v oblaku.** Za srednja podjetja, ki so navajena na popoln pregled in nadzor nad svojim celotnim IT sistemom, lahko že prenos nekaterih komponent na oblak povzroči operacijske slabosti, pri katerih napake oz. prekinitve storitev niso takoj vidne.

- **Komunikacija na virtualni ravni.** Virtualne naprave morajo komunicirati in med seboj deliti podatke. Če ta komunikacija ne temelji na varnosti, obstaja nevarnost, da komunikacija postane tarča napadov. [10]

Napadi

Danes je v IT svetu veliko napadov. Kakor lahko oblak uporabljajo zakoniti uporabniki, pa ga lahko izkoristijo tudi napadalci, ki imajo zlonamerne namene. Napadalec lahko oblak uporabi kot gostitelja za zlonamerno aplikacijo, da doseže svoj namen (npr. DDoS napad na sam oblak) ali dodeli oblaku drugega uporabnika. Če

napadalec ve, da njegova žrtev uporablja storitve ponudnika oblaka z imenom X, lahko napadalec s podobnim ponudnikom storitve oblaka simulira napad na svojo žrtev. Ta situacija je podobna scenariju, ko sta tako napadalec kot žrtev v enakem omrežju, a namesto fizičnega omrežja uporabljata različne virtualne naprave (Slika 3.6). [10]



Slika 3.6: Scenarij napada znotraj oblaka. [10]

DDoS napadi (porazdeljena ohromitev storitve)

Pri tem napadu ima napadalec pod seboj ostale naprave, ki sledijo njegovim ukazom. Ko napadalec z ukazom sporoči ostalim napravam, naj ohromijo določeno napravo, te običajno zasujejo virtualne naprave z veliko količino IP paketov na določena omrežna vrata. [10]

V računalništvu v oblaku, kjer si infrastrukturo deli veliko število uporabnikov virtualnih naprav, imajo lahko DDoS napadi večji učinek kot pri arhitekturi z enim uporabnikom.

DDoS zaščita je del ravni omrežne virtualizacije in ne strežniške virtualizacije. Oblačni sistemi, ki uporabljajo virtualne naprave, se lahko zavzamejo z ARP slepljenjem na ravni omrežja. Slepljenje ARP vključuje pošiljanje lažnih ARP odgovorov napravi v omrežju. Naprava, ki je tarča tovrstnega napada, bo imela posledično neustrezno ARP tabelo in Ethernet bo zaradi tega posredoval okvirje napačni napravi. [17]

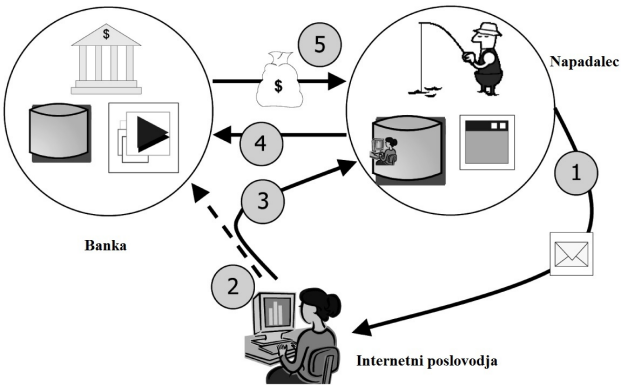
Omrežje mora biti dobro varovano; treba je imeti več požarnih zidov in izenačevalnikov obremenitev. [10]

Napadi odjemalec-odjemalec

Zlonamerna virtualna naprava lahko okuži vse virtualne naprave, ki so nameščene na fizičnem strežniku. Napad na enega odjemalca oz. virtualno napravo se lahko razširi na druge virtualne naprave, ki gostujejo na istem fizičnem strežniku. To je največje varnostno tveganje v virtualnem okolju. Ko se zlonamerni uporabnik osredotoči na virtualne naprave, te lahko postanejo dostopne tudi ostalim. Tako lahko napadalec prek te virtualne naprave okuži tudi ostale. Na ta način se izogne hipervizorju in dobi dostop do ravni okolja, ki uradno ni dostopna z ravni virtualne naprave. Največje tveganje v virtualnem okolju so ravno napadi "odjemalec-odjemalec". Pri takšnem napadu dobi napadalec administratorske pravice za infrastrukturno raven virtualnega okolja in lahko dostopa do vseh virtualnih naprav. Če dobi napadalec nadzor nad hipervizorjem, nadzoruje tudi vse podatkovne prenose med hipervizorjem in virtualnimi napravami. [10]

Napadalec lahko izvede tudi napad lažnega predstavljanja (ang. *phishing attack*), kot je prikazano na sliki 3.7:

1. Napadalec se pretvarja, da je banka, in pošlje poslovodji zahtevo za vnos dostopnih podatkov do bančnega računa.
2. Prikaz povezave med poslovodjo in banko (vendar se povezava ne izvede).
3. Poslovodja pošlje napadalcu svoje dostopne podatke bančnega računa.
4. Napadalec izvede transakcijo v imenu poslovodje.
5. Napadalec prejme transakcijo z bančnega računa poslovodje.



Slika 3.7: Napad z lažnim predstavljanjem. [11]

Poglavje 4

Stikala

4.1 LAN stikalo

Na področju omreženja je stikalo visoko hitrostna naprava, ki sprejema vstopne podatkovne pakete, in jih usmerja do njihovih destinacij na lokalnem omrežju (ang. *local area network*). LAN stikalo deluje na povezovalni plasti (plasti 2) ali na omrežni plasti (plasti 3) OSI modela in tako podpira vse tipe paketnih protokolov. [12]

Slika 4.1: LAN stikalo. [13]

4.2 Virtualno stikalo

Virtualno stikalo ali kratko vStikalo [14] predstavlja omrežne entitete, ki povezujejo virtualne naprave v virtualnem omrežju na ravni 2. VStikalo ne posreduje le podatkovnih paketov, ampak pametno preklaplja komunikacije v omrežju, tako da preveri podatkovne pakete preden jih premakne do njihove destinacije.

Virtualna stikala so po navadi vgrajena v nameščeno programsko opremo, lahko pa so tudi vključena v strojno opremo strežnika, kot del njegove strojno-programske opreme. Virtualno stikalo združuje fizična stikala v eno logično stikalo. To poveča pasovno širino in ustvari učinkovitejše omrežje med strežniki in stikali.

Namen virtualnega stikala je, da zagotovi mehanizem za zmanjšanje kompleksnosti omrežne konfiguracije. To se doseže z upravljanjem in zmanjševanjem števila stikal. Ker je virtualno stikalo pametno, lahko zagotovi varnejše virtualne naprave, ki vključujejo omrežne in varnostne nastavitve. To se je izkazalo za veliko pomoč omrežnim administratorjem, saj je selitev virtualnih naprav po fizičnem gostitelju zamudna in predstavlja varnostno tveganje. [15]

Virtualno stikalo ima nekaj ključnih prednosti:

- pomaga pri lažji postavitvi in selitvi virtualnih strežnikov.
- omrežnim administratorjem omogoča upravljanje virtualnih stikal, ki so bila postavljena prek hipervizorja,
- v primerjavi s fizičnim stikalom je pri virtualnem stikalu lažje vpeljati novo funkcionalnost, ki je lahko povezana tako s strojno kot s strojno-programsko opremo. [14]

4.2.1 Delovanje virtualnega stikala

Virtualno stikalo je "sestavljeno po naročilu" iz manjših funkcionalnih enot. [16]

Nekatere izmed glavnih funkcionalnih enot pa so:

- glavna posredovalna naprava plasti 2. Ta je ključni element sistema (tako za zmogljivost kot za točnost), ki je v virtualni infrastrukturi še poenostavljena, tako da obdeluje samo Ethernet glave na plasti 2. Je popolnoma neodvisna od drugih izvedbenih podrobnosti, kot so razlike v fizičnih Ethernet adapterjih in razlike v posnemanju pri virtualnih Ethernet adapterjih.
- VLAN enote za označevanje, odstranjevanje in filtriranje.
- Varnost plasti 2, kontrolna vsota in enote za prenos segmentacije.

Ta modularni pristop je postal osnovno načelo v prihodnjem razvoju. Ko se v času delovanja virtualno stikalo vgradi, strežnik naloži samo tiste komponente,

ki jih potrebuje. Namesti in zažene le to, kar je dejansko potrebno za podporo določenim fizičnim in virtualnim tipom Ethernet adapterjev, ki so uporabljeni pri konfiguraciji. To pomeni, da sistem za sistemsko zmogljivost predstavlja minimalno kompleksnost in zahteve.

Virtualna stikala strežnika so v več pogledih podobna fizičnim stikalom. Obstajajo pa tudi nekatere pomembne razlike. [16]

Delovanje virtualnega stikala v primerjavi s fizičnim stikalom

Virtualno stikalo, ki je uporabljeno v virtualnem strežniku, deluje zelo podobno kot moderno Ethernet stikalo. [16] Vzdržuje posredovalno tabelo z MAC vrati in izvaja naslednje funkcije, kot so:

- preveri ciljni MAC vsakega okvirja, ko ta prispe,
- posreduje okvir k enim ali več vratom za prenos,
- izogiba se nepotrebnim dostavam (z drugimi besedami, ne gre za hub (razdelilnik)).

Virtualno stikalo strežnika podpira VLAN segmentacijo na ravni vrat. To pomeni, da je pri konfiguraciji vrat mogoče izbrati enega od naslednjih načinov:

- z dostopom do enega VLANa, ki v svetu fizičnih stikal prevzame vlogo tako imenovanih dostopnih vrat, oz. v terminologiji virtualnega strežnika, označuje virtualno stikalo,
- z dostopom do več VLANov, pri čemer se značke ne spreminjajo, kar v svetu fizičnih stikal prevzame vlogo tako imenovanih povezovalnih vrat oz,. v terminologiji virtualnega strežnika, označuje virtualne goste.

Virtualno stikalo strežnika podpira kopiranje paketov k preslikovalnim vratom. Z uporabo tako imenovanega promiskuitetnega načina, virtualni strežnik določi, da vrata virtualnega stikala delujejo kot SPAN ali preslikovalna vrata. Ta zmogljivost omogoča popravljanje napak s pomočjo vohljača ali z zagonom aplikacij, kot je IDS.

Virtualni strežnik [16] za konfiguracijske podatke, kot so veljavne posodobitve za MAC filtre, zagotavlja neposreden kanal od virtualnih Ethernet adapterjev.

Tako ni potrebe za učenje unicast naslovov oz. izvajanje IGMP sledenja za učenje skupinskega članstva za oddajanje na več naslovov (ang. *multicast*).

Vrata na virtualnem stikalu lahko samodejno preidejo v preslikovalni način, ko je virtualni adapter postavljen v promiskuitetni način. Pri tem pa morata virtualno stikalo in politika skupine vrat to dovoliti. [16]

4.2.2 Izolacija virtualnega stikala

Omrežni promet zaradi izolacije ne more potekati neposredno od enega virtualnega stikala do drugega virtualnega stikala znotraj istega gostitelja, ker deluje na programskem nivoju. Virtualna stikala zagotavljajo vsa vrata, ki jih potrebuje ponudnik oblaka v enem stikalu, kar ima naslednje prednosti: [16]

- ker ni potrebe za kaskadno razporeditev virtualnih stikal, virtualna infrastruktura ne omogoča povezav virtualnih stikal,
- ker virtualnih stikal ni mogoče povezati, ni potrebe za preprečitev slabih povezav virtualnih stikal,
- ker si virtualna stikala ne morejo deliti fizičnih Ethernet adapterjev, Ethernet adapterja nikakor ni mogoče pripraviti do povratne zanke ali kakšne podobne konfiguracije, ki bi povzročila uhajanje med virtualnimi stikali.

Poleg tega ima vsako virtualno stikalo [16] svojo posredovalno tabelo in ni mehanizma, ki bi dovolil vstop do ene tabele in usmeril do vrat na drugem virtualnem stikalu. Vsaka destinacija, ki jo stikalo poišče, se lahko ujema samo z vrati na istem virtualnem stikalu, iz katerega je okvir, tudi če iskalne tabele drugih virtualnih stikal vsebujejo vhode za ta naslov.

Majhna verjetnost je, da bi lahko potencialni napadalec obšel izolacijo virtualnega stikala. To bi bilo mogoče samo v primeru velike in neznane varnostne vrzeli v jedru. Ker virtualni strežnik razčleni tako malo podatkov iz okvirja (v glavnem samo Ethernet glave), bi bilo to težko, poleg tega pa so, ko napadalec že ima dostop, na voljo bolj pomembne tarče, kot npr. prekinitev izolacije virtualnega stikala.

Za izolacijo obstajajo naravne ovire. Če povežemo povezave navzgor dveh virtualnih stikal oz. če se povežeta dve virtualni stikali s programi, ki se izvajajo na virtualni napravi, lahko pride do enakih težav kot pri fizičnih stikalih. [16]

4.2.3 Virtualna vrata

Vrata na virtualnem stikalu [16] zagotavljajo logične povezovalne točke med virtualnimi napravami in med virtualnimi in fizičnimi napravami. Lahko si jih predstavljamo kot virtualne RJ-45 konektorje. Vsako virtualno stikalo ima lahko do 1.016 virtualnih vrat. Na vseh virtualnih stikalih gostitelja je do 4.096 vrat.

Virtualna vrata na virtualnem strežniku zagotavljajo neprecenljiv nadzorni kanal za komunikacijo z virtualnimi Ethernet adapterji, ki so na njih priključeni.

Naloge virtualnih vrat virtualnega strežnika:

- zanesljivo vedo, kateri so konfigurirani sprejemni filtri za Ethernet adapterje, ki so na njih priključeni. To pomeni, da se za shranjevanje posredovalnih tabel ni treba učiti MACov.

- Za razliko od fizičnih stikal zanesljivo poznajo zapleteno konfiguracijo virtualnih Ethernet adapterjev, ki so priključeni na njih. To omogoča postavitev politike kot npr. "gost ne more spreminjati MAC naslova", saj vrata virtualnega stikala v osnovi zagotovo vedo, kaj je "zapečeno na pomnilniku" (pravzaprav shranjeno v konfiguracijski datoteki, zunaj nadzora operacijskega sistema gosta). [16]

4.2.4 Pravilnost virtualnega stikala

Pomembno je, da zagotovimo, da virtualne naprave [16] oz. druga vozlišča ne morejo vplivati na vedenje virtualnega stikala. Virtualni strežnik varuje pred vplivi na naslednje načine:

- virtualna stikala se, da bi naselila svoje posredovalne tabele, ne učijo od omrežja. Pri tem se izloči potencialni vektor za zavrnitev storitve (ang. *leakage attack*) kot neposredni poskus zavrnitve storitve oz. bolj verjetno kot stranski učinek kakšnega drugega napada, npr. črva ali virusa, saj išče gostitelje, ki se jih da zlahka napasti.

- Virtualna stikala naredijo zasebne kopije vseh okvirnih podatkov, ki so uporabljeni pri odločitvah za posredovanje oz. filtriranje. To je kritična in edinstvena funkcija virtualnega stikala.

Virtualno stikalo ne kopira celotnega okvirja, saj bi bilo to neučinkovito. Virtualni strežnik mora poskrbeti za to, da operacijski sistem gosta nima dostopa do kakršnih koli občutljivih podatkov, ko se okvir posreduje virtualnemu stikalu.

Virtualni strežnik zagotavlja, da se okviri nahajajo v primernem VLANu na virtualnem stikalu. Proces poteka na naslednje načine:

- VLAN podatki se prenesejo zunaj okvirja, ko preidejo čez virtualno stikalo. Filtriranje je preprosta celoštevilčna primerjava. To je le posebni primer splošnega načela, zakaj sistem ne bi smel zaupati podatkom, dostopnim uporabniku.
- Virtualna stikala nimajo dinamične združevalne podpore.

Dinamično združevanje in prikrojeni VLAN so funkcije, pri katerih lahko napadalec najde šibke točke, ki lahko odprejo varnostne vrzeli izolacije. To ne pomeni, da te funkcije same po sebi niso varne, ampak lahko njihova kompleksnost, tudi če so varno implementirane, vodi do napačne konfiguracije in odpre napad vektorju. [16]

Poglavje 5

Prednosti in slabosti

5.1 Zasebni oblak

5.1.1 Prednosti storitve zasebnega oblaka

Storitev zasebnega oblaka ima vrsto prednosti: [8]

- **Boljši nadzor.** Ker se programska oprema nahaja na lokaciji uporabnika, imajo organizacije boljši nadzor nad svojimi podatki. Organizacija je odgovorna za upravljanje in vzdrževanje podatkov, kar omogoča popoln pregled nad podatki.

- **Boljša varnost.** Ker so storitve zasebnega oblaka namenjene samo eni organizaciji, se lahko programska oprema, pomnilniki podatkov in omrežja oblikujejo tako, da zagotavljajo visoko raven varnosti, tako da drugi uporabniki istega podatkovnega središča do njih nimajo dostopa. To ne pomeni, da storitev javnega oblaka ni varna. Gre le za to, da imajo nekatera podjetja raje, če njihovi podatki ostanejo na njihovi lokaciji. Zasebni oblak je lahko bolj privlačen tudi zaradi regulativnega okvirja posamezne države. V nekaterih državah se mora podatkovno središče, ki gosti storitev javnega oblaka, nahajati v državi uporabnika storitve. Kjer ni možnosti javnega oblaka, ki

bi ga ponudila država, je zasebni oblak edina možna izbira.

- **Višja zmogljivost.** Zasebni oblak se postavi znotraj požarnega zidu na intranet organizacije, kar pomeni, da se hitrost prenosa, v primerjavi z uporabo interneta, občutno poveča. Poleg tega ni težav s počasnim dostopom do spletnih strani, kar lahko predstavlja težavo pri storitvi javnega oblaka.

- **Večja skladnost.** Podatki o skladnosti Sarbannes Oxley, PCI DSS in HIPAA so lahko dostavljeni pri postavitvi javnega oblaka, a včasih podatki niso tako podrobni ali prilagodljivi. Ker so strojna oprema, pomnilnik in konfiguracija omrežja namenjeni enemu uporabniku, je podatke o skladnosti veliko lažje pridobiti in redno preverjati.

- **Prilagodljivost.** Zmogljivost strojne opreme, omrežja in pomnilnika se lahko pri zasebnem oblaku podrobno določi in prilagodi, saj je ta v lasti podjetja.

Kot smo prikazali zgoraj, več nadzora s strani uporabnika storitve zasebnega oblaka pomeni manj skrbi glede varnosti. S premikom tradicionalnega strojno podprtega IT sistema k oblaku lahko uporabnik še zmeraj uživa v prednostih posodobitev, prilagodljivosti in večji produktivnosti, ne da bi se zaradi tega moral odreči odgovornosti za varnost podatkov kot v nekaterih primerih pri storitvi javnega oblaka. [8]

5.1.2 Slabosti storitve zasebnega oblaka

Medtem ko so prednosti zasebnega oblaka večji nadzor in varnost, je treba razmisliti tudi o slabostih. [8]

- **Višji stroški.** Storitve zasebnega oblaka so običajno dražje kot storitve javnega oblaka, saj so potrebni tako strojna oprema kot osebje za vzdrževanje.

Za izgradnjo storitve zasebnega oblaka mora organizacija investirati v strojno opremo ali uporabiti obstoječe sisteme, medtem ko se storitev javnega oblaka upravlja izven lokacije uporabnika. Zasebni oblaki prav tako zahtevajo upravljavce sistema, kar pomeni višje administracijske stroške.

- **Lastno vzdrževanje.** Ker vzdrževanje zasebnega oblaka poteka na lokaciji podjetja, mora organizacija zagotoviti zadostno energijo, hlajenje in splošno vzdrževanje na lokaciji podjetja. Še večji strošek pa predstavlja ustrezno število zaposlenih z ustreznim znanjem in izkušnjami. Organizacija gostiteljica mora upoštevati možnost izgube podatkov zaradi fizične poškodbe na enoti (npr. požar, nihanje napetosti, škoda zaradi vode). Če ima podjetje več podatkovnih središč in ima vsako središče zasebni oblak, se stroški za vzdrževanje na lokaciji uporabnika in vsi s tem povezani stroški skokovito povečajo.

- **Meja zmogljivosti.** Zaradi omejitev strojne opreme v podatkovnih središčih podjetja bo zmeraj obstajala meja zmogljivosti. Znotraj okolja podjetja je na primer na voljo le toliko prostora, da se lahko postavi samo določeno število strojnih strežnikov.

Največja slabost storitve zasebnega oblaka je ta, da mora uporabnik kupiti, konfigurirati in vzdrževati sistem ali virtualno infrastrukturo. Medtem ko uporabnik storitve javnega oblaka lahko kupi poceni že pripravljen sistem, ki ga lahko uporabi takoj, mora uporabnik zasebnega oblaka na začetku investirati znatne vsote denarja za nakup sistema, ki bo večinoma gostoval na njegovi lokaciji, in hkrati poskrbeti za njegovo redno vzdrževanje. To je treba vzeti v zakup za višjo varnost in nadzor, ki ga nudi storitev zasebnega oblaka. [8] Varnost je višja samo v primeru, da imamo dovolj dobre varnostne strokovnjake.

5.2 Javni oblak

5.2.1 Prednosti storitve javnega oblaka

Pri odločitvi med javnim in zasebnim oblakom mora podjetje upoštevati določene prednosti in slabosti. Prednosti storitve javnega oblaka so naslednje: [8, 19]

- **Preprostost in učinkovitost.** To sta glavni prednosti javnega oblaka. Javni oblak je na voljo kot storitev, običajno prek internetne povezave. Tretji ponudnik storitve zunaj lokacije je gostitelj in upravljavec sistema. Uporabniki se s sistemom povežejo prek interneta. Pri javnih oblakih se po navadi zaračuna mesečna oz. letna pristojbina za uporabo storitve.

- **Varnostno kopiranje in obnovitev.** Podatki, ki se jih vzdržuje v oblaku, so bolj dosegljivi, hitreje jih je mogoče obnoviti in v številnih okoliščinah so bolj zanesljivi kot ti v tradicionalnih podatkovnih centrih. Storitve oblaka se lahko uporabijo kot sredstvo za varno shranjevanje podatkovnega centra izven podjetja. Zmogljivost omrežja prek interneta in količina podatkov sta omejujoča dejavnika, ki lahko vplivata na obnovitev.

- **Podatkovni center.** Storitve oblaka se lahko uporabijo za večjo varnost podatkovnega centra. Na primer elektronska pošta lahko poteka prek ponudnika oblaka, kjer se pregleda in analizira skupaj s podobnimi prenosi iz drugih podatkovnih centrov za odkrivanje nezaželene pošte, lažnega predstavljanja, zlonamernih kampanj in za bolj celostno izvajanje sanacijskih ukrepov (npr. izolacija sumljivih sporočil in vsebine). Raziskovalci so prav tako uspešno predstavili sistem za zagotovitev protivirusnih storitev, zasnovanih na oblaku, kot alternativo protivirusnim rešitvam.

- **Nizki stroški.** Ob odločitvi za storitev javnega oblaka lahko organizacije zmanjšajo proračun za IT, saj so strežniki virtualni in jih gosti tretja oseba. Organizacijam ni treba kupiti strojne opreme (kar pomeni prihranek

pri stroških za energijo). Organizacije si lahko prikrojijo storitev javnega oblaka s posebnimi možnostmi (npr. število uporabnikov), tako da plačajo samo to, kar potrebujejo (plačilo po porabi). Ker je gostitelj javnega oblaka tretja oseba, organizaciji ni treba zapravljati denarja za zaposlitev IT upravljavca sistema; za to poskrbi gostitelj.

- **Krajši čas.** Vzdrževanje internih strežnikov zahteva čas. Če je treba spremeniti konfiguracijo strojne ali programske opreme oz. če se strežnik zruši ali ga je treba ponovno zagnati, lahko takšen proces, odvisno od situacije, traja več ur oz. več dni. Zaradi virtualnega značaja storitve javnega oblaka, ponovna konfiguracija oblaka traja le nekaj minut. Ker strežniki gostujejo v oblaku, se lahko, če strežnik odpove, takoj aktivira drug strežnik, kar skrajša čas izpada.

- **Mobilnost.** Odjemalci oblaka lahko delujejo prek brskalnika ali aplikacije. Ker so glavni računalniški viri, ki so potrebni, shranjeni s strani ponudnika oblaka, so odjemalci običajno v računalniškem smislu manj obremenjeni in jih je na prenosnih računalnikih, kot tudi na vgrajenih napravah, kot so pametni telefoni, tablični računalniki in osebni organizatorji, zlahka podpreti.

- **Brez vzdrževanja.** Ker je gostovanje javnega oblaka izven uporabnikove lokacije, interni IT upravljavci niso odgovorni za upravljanje sistema. Dizajn uporabniku omogoča hitrejšo posodobitev oz. vpeljavo tehnologije v sistem, saj vse upravlja gostitelj storitve. Pri storitvi javnega oblaka nikoli ni treba skrbeti za strojno opremo; upravljanje poteka prek preprostega nastavitvenega zaslona.

- **Brez pogodb.** Če so podatki javnega oblaka v takšni obliki, da jih lahko brez težav izvozimo k drugemu gostitelju, potem s ponudnikom javnega oblaka nimamo dolgoročnih obveznosti. Ko se uporabnikova mesečna oz. letna naročnina izteče, ni zavezan k nadaljnji uporabi storitve javnega oblaka.

Kar zadeva nadgradnjo, večnamenskost, preprostost uporabe in ceno, ima storitev javnega oblaka po navadi prednost pred storitvijo zasebnega oblaka. Večina podjetij kot glavne prednosti storitve javnega oblaka navaja možnost uporabe vseh storitev, vključno z infrastrukturo na osnovi plačila po porabi, ter odsotnost težav, povezanih z njihovim dnevnim upravljanjem. [8, 19]

5.2.2 Slabosti storitve javnega oblaka

Slabosti storitve javnega oblaka so naslednje: [8, 19, 20]

- **Pomanjkanje nadzora.** Ker podatkovni sistem nadzoruje tretji ponudnik, ima veliko podjetij občutek, da z javnim oblakom nimajo dovolj nadzora nad svojimi osebnimi podatki.

- **Kompleksnost sistema.** Računalniško okolje javnega oblaka je v primerjavi s tradicionalnimi podatkovnimi centri zelo kompleksno. Javni oblak sestavlja veliko komponent, zato je površina za napad velika. Poleg komponent za splošno računalništvo, kot npr. nameščene aplikacije, monitorji virtualnih naprav, monitorji virtualnih naprav gostiteljev, monitorji podatkovnih centrov in monitorji podporne vmesne opreme, so v javnem oblaku tudi komponente, ki imajo nad vsemi temi nadzor. Poznamo več vrst komponent za upravljanje, kot so npr. komponente za samopostrežne storitve, komponente za obračun uporabe virov po porabi, komponente za upravljanje kvot, komponente za podvojevanje in obnovitev podatkov, komponente za upravljanje delovne obremenitve in komponente za razširitev oblaka. Storitve oblaka lahko izvedemo tudi z gnezdenjem storitev drugih ponudnikov oblaka. Komponente se s posodobitvami in izboljšavami spreminjajo, kar stvari še dodatno oteži. Varnost je odvisna ne samo od pravilnih in učinkovitih komponent, ampak tudi od njihovega medsebojnega delovanja. Število možnih interakcij med komponentami se poveča za kvadrat števila komponent, kar zviša stopnjo kompleksnosti. Kompleksnost je obratno sorazmerna z varnostjo, kar pomeni, da je z večjo kompleksnostjo sistem tudi bolj ranljiv.

- **Nizka hitrost.** Storitve javnega oblaka so zasnovane na spletnih povezavah, kar pomeni, da je hitrost prenosa podatkov odvisna od ponudnika internetnih storitev. Če podjetje shranjuje oz. prenaša velike količine podatkov oz. zahtevkov, storitev javnega oblaka mogoče ni najboljša rešitev. Poleg tega morajo strežniki javnega oblaka uporabnikom zagotoviti hiter dostop do njihovih podatkov.

- **Okolje z več odjemalci.** Pri storitvah javnega oblaka, ki jih ponujajo ponudniki, se naročniki soočijo z resno težavo, ker običajno delijo komponente in vire z drugimi naročniki, ki jih ne poznajo. Vsako leto je več nevarnosti za omrežje in za računalniško infrastrukturo, tako ta postaja bolj kompleksna. Deljenje infrastrukture z nepoznanimi zunanjimi strankami je lahko za nekatere aplikacije velika slabost in zahteva visoko stopnjo zagotovila moči varnostnih mehanizmov, ki se uporabljajo za logično delitev. Logična delitev, ki se ne uporablja samo pri računalništvu v oblaku, ni nepomemben problem, saj dobi z obsegom računalništva v oblaku še dodatne razsežnosti. Dostop do korporativnih podatkov in virov bi lahko bil s konfiguracijo ali napako programske opreme nenamerno izpostavljen drugim naročnikom. Napadalec bi se lahko tudi izdajal za naročnika, tako da bi izkoristil šibke točke znotraj okolja oblaka in pridobil nepooblaščen dostop.

- **Pomanjkanje naložb.** Kljub temu da zmanjšanje potrebe po predhodnih naložbah pomeni velik prihranek, je najem storitev zunanjega ponudnika hkrati slaba naložba. Predmeti v interni lasti, kot npr. strežniki ali omrežna oprema, se v obliki premoženja in davčnih prednosti na dolgi rok obrestujejo.

- **Izguba nadzora.** Obstaja kar nekaj pomislekov glede zunanjega nadzora korporativnih sredstev in možnega napačnega upravljanja. Prehod na javni oblak zahteva prenos nadzora podatkov in sistemskih komponent (nad katerimi je imelo neposredni nadzor podjetje samo) na ponudnika oblaka. Izguba nadzora, tako nad fizičnimi kot tudi logičnimi vidiki sistema in podatkov zmanjša sposobnost podjetja, da ohrani pregled nad položajem, pretehta alternative, določi prednosti in vpliva na spremembe v varnosti in zasebnosti.

Kot pri vsaki tehnologiji, so lahko tudi storitve računalništva v oblaku v prid napadalcem.

- **Botneti ali omrežja robotskih računalnikov.** Omrežja robotskih računalnikov so omrežja, ki jih zberejo in nadzirajo napadalci. Omrežja robotskih računalnikov se lahko uporabljaljajo za pošiljanje nezaželene pošte, prestrezanje prijavnih podatkov (npr. uporabniških imen in gesel) ter za izvajanje napadov z vrinjenjem na spletne strani. Botneti se lahko tako uporabljajo za ohromitev storitve v infrastrukturi ponudnika oblaka.

- **Opazno slabša varnost.** Glavna slabost storitve javnega oblaka je ravno slaba varnost. To ne pomeni, da javni oblak ni varen – večina javnih oblakov ima odlične varnostne ukrepe. A za uporabnike z občutljivimi osebnimi podatki (npr. finančne ustanove), je predstava, da morajo te informacije zaupati tretji osebi, pogosto nesprejemljiva in obremenjujoča. [8, 19]

Najpogostejše nevarnosti v javnem oblaku

Da bi identificirali in pridobili strokovno mnenje o največjih nevarnostih znotraj računalništva v oblaku, so pri nevladni organizaciji CSA (ang. *Cloud Security Allience*) strokovnjaki s tega področja izvedli raziskavo in prikazali devet največjih nevarnosti. [20]

Nevarnosti, ki se pojavljajo v javnem oblaku, so predstavljene po vrstnem redu od največje do najmanjše:

- kršitev varnosti podatkov,
- izguba podatkov,
- ugrabitev računa ali prometa storitve,
- nezanesljivi uporabniški in programski vmesniki,
- zavrnitev storitve,
- notranji napadalec,
- zloraba storitve oblaka,

- nezadosten pregled in
- skupne tehnološke ranljivosti.

Kršitev varnosti podatkov. Izguba in uhajanje podatkov sta v računalništvu v oblaku resen problem. Podatke sicer lahko šifriramo, ampak ob izgubi šifrirnega ključa, izgubimo celotne podatke. V kolikor se odločimo, da varnostnih kopij ne bomo hranili samo na spletu (na ta način zmanjšamo možnost izgube podatkov), smo izpostavljeni kršitvam o varnosti podatkov.

Izguba podatkov. V skladu s pravili Evropske unije o varovanju podatkov, se uničenje podatkov obravnava kot kršitev, ki zahteva ustrezno prijavo. Mnoge politike tako od podjetij zahtevajo, da pridobijo revizijske zapise in drugo potrebno dokumentacijo. Če podjetje te podatke hrani v oblaku, lahko izguba teh ogrozi poslovanje v podjetju.

Ugrabitev računa ali prometa storitve. Ugrabitev računa in storitve, običajno z ukradenimi poverilnicami, ostaja največja nevarnost. Z ukradenimi poverilnicami lahko napadalci dostopajo do kritičnih področij v storitvi računalništva v oblaku, kar jim omogoča, da ogrozijo zaupnost, integriteto in dostopnost teh storitev. Podjetja bi morala poznati splošne zaščitne strategije za zajezitev škode, ki jo kršitev povzroči. Podjetja bi morala preprečiti izmenjavo uporabniških poverilnic med uporabniki in storitvami ter izkoristiti zelo dobro tehniko avtentikacije z dvema faktorjema, kjerkoli je to mogoče.

Nezanesljivi uporabniški in programski vmesniki. Medtem ko večina ponudnikov skrbi za zagotavljanje varnosti in to tudi vgradi v svoj model storitve, je za uporabnike storitev odločilnega pomena, da so seznanjeni z varnostjo, uporabo, upravljanjem, organizacijo in nadzorom storitev v oblaku. Zanašanje na uporabniške vmesnike in programske vmesnike podjetje izpostavi mnogim dilemam o varnosti, zaupnosti, integriteti, dostopnosti in odgovornosti.

Zavrnitev storitve. Izpad storitve uporabniku onemogoči delovanje, zato se sprašuje, ali se je selitev pomembnih podatkov na oblak zaradi manjših stroškov infrastrukture res obrestovala. Še huje, ker ponudniki oblaka uporabnikom storitev

pogosto zaračunajo na podlagi računalniških ciklov in porabljenega prostora na disku, obstaja možnost, da napadalec storitvi ne bo mogel v celoti onemogočiti dostopa do omrežja, in bo tako povzročil veliko porabo procesnega časa. S tem bo storitev postala predraga za uporabnika in jo bo ta prisiljen prekiniti sam.

Notranji napadalec. Zlonamerni notranji napadalec, kot npr. skrbnik sistema, ima lahko pri neprimerno oblikovanem oblaku dostop do potencialno občutljivih podatkov. Zlonamerni notranji napadalec ima vedno večji dostop do ključnih sistemov (od infrastrukture kot storitve do platforme kot storitve in do programske opreme kot storitve) ter navsezadnje do podatkov. Sistemi, ki se glede varnosti zanašajo samo na ponudnika storitve oblaka, so izpostavljeni velikemu tveganju. Sistem je izpostavljen napadu zlonamernega napadalca tudi v primeru uporabe šifriranja, in sicer, če uporabnik šifrirnega ključa ne hrani sam oz. če ta ni na voljo samo v času uporabe podatkov.

Zloraba storitve oblaka. Ta nevarnost, bolj kot za uporabnike oblaka, predstavlja težavo za ponudnike storitve oblaka. Zastavljajo se številna pomembna vprašanja: kako bomo odkrili ljudi, ki zlorabljajo storitev; kako bomo zlorabo definirali; kako bomo preprečili, da se zloraba ne ponovi?

Nezadosten pregled. Podjetje, ki se v naglici odloči za tehnologijo oblaka, je izpostavljeno mnogim težavam. Zaradi neskladnih pričakovanj med ponudnikom storitve oblaka in uporabnikom, se pojavljajo vprašanja o pogodbeni obveznosti, odzivu in transparentnosti. Postavitev aplikacij na oblak, ki so odvisne od "notranjih" nadzornih mehanizmov omrežne varnosti, predstavlja nevarnost, v kolikor so ti mehanizmi odstranjeni oz. se ne ujemajo s pričakovanji uporabnika. Postavljajo se vprašanja glede delovanja in oblikovanja, ko aplikacijo, ki naj bi bila postavljena na oblak, urejajo posamezniki, ki se na tehnologijo oblaka ne spoznajo. Podjetja in institucije, ki se odločijo za model tehnologije oblaka, morajo torej imeti zmogljive vire in izvajati obsežen notranji in zunanji pregled.

Skupne tehnološke ranljivosti. Vgrajena skupna tehnologija, kot je hipervizor, skupna komponenta platforme in aplikacija v okolju "programske opreme kot storitve", predstavljajo grožnjo tako uporabniku, kot tudi celotnemu okolju. Ta izpostavljenost je nevarna, saj vpliva na oblak v celoti. [20]

Poglavje 6

Sklep in ugotovitve

To diplomsko delo preučuje zasebni in javni oblak. Raziskali smo nevarnosti, ki pretijo v obeh vrstah oblakov, in na kaj moramo biti pozorni, ko se odločamo za posamezen oblak.

V prvem delu smo predstavili računalništvo v oblaku, vrste oblakov in storitvene modele javnega oblaka. V osrednjem delu smo opisali različne vrste virtualizacij: virtualizacijo strežnika, virtualizacijo shranjevanja, virtualizacijo omrežja in virtualizacijo storitve. Predstavili smo upravljanje omenjenih virtualizacij. V naslednjem koraku smo se osredotočili na povezavo med zanesljivostjo in varnostjo virtualizacij. Opisali smo varnost virtualnih naprav ter nevarnosti in napade, ki so možni pri virtualizaciji.

V zadnjem delu diplomske naloge smo predstavili upravljanje stikal v virtualizaciji, delovanje virtualnega stikala, izolacijo virtualnega stikala, virtualna vrata in pravilnost virtualnega stikala.

Na koncu diplomskega dela smo natančno analizirali prednosti in slabosti zasebnega in javnega oblaka. Naj naštejemo nekaj prednosti zasebnega oblaka: boljši nadzor, boljša varnost, prilagodljivost in večja skladnost. Med prednosti javnega oblaka pa sodijo denimo nizki stroški, mobilnost, odsotnost vzdrževanja strežnikov ter varnostno kopiranje in obnovitve.

Namen diplomske naloge je bil prikaz obeh vrst oblakov. Uporabnik se na podlagi ugotovitev v diplomski nalogi lažje odloči, na kateri oblak preiti. Podrobni opisi prednosti in slabosti zasebnega in javnega oblaka ter prikaz nevarnosti, ki so možne v virtualizaciji, uporabnika vodijo do prave odločitve.

Menimo, da bodo ljudje v prihodnosti bolj prehajali na javni oblak, saj je ta cenejši in fleksibilnejši, poleg omenjenega pa je vzdrževanje samega oblaka v rokah ponudnika in je uporabnik bolj brezskrben. Obstaja težava z zaupnimi podatki, nad katerimi uporabnik nima nadzora. Sami bi izbrali zasebni oblak, vendar ta ni tako fleksibilen in cenovno ugoden. Alternativna rešitev bi bila izbira hibridnega oblaka, kjer bi zaupne podatke še vedno shranjevali na lokalnih strežnikih, ostale storitve pa bi zakupili v javnem oblaku.

Literatura

[1] The NIST Definition of Cloud Computing (september, 2011). *NIST National Institute of Standards and Technology*. Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] (2014) Računalništvo v oblaku. Dostopno na: http://www.esistemi.si/raunalnitvo-v-oblaku.

[3] (2011) Miha Puš, *Identifikacija potrebne opreme za izdelavo privatnega oblaka*, diplomsko delo. Dostopno na: http://eprints.fri.uni-lj.si/1352/1/Pu%C5%A1_M.1.pdf.

[4] (2011) Kaj je sploh računalništvo v oblaku. Dostopno na: http://www.mojmikro.si/center/povem_naglas/kaj_je_sploh_racunalnistvo_v_oblaku.

[5] (2014) Javni oblaki. Dostopno na: http://student.fnm.uni-mb.si/~zmocivnik/index.php?option=com_content&view=article&id=71&Itemid=89.

[6] (2014) Hibridni oblaki. Dostopno na: http://student.fnm.uni-mb.si/~zmocivnik/index.php?option=com_content&view=article&id=73&Itemid=91.

[7] V. Josyula, M. Orr, G. Page, *Cloud Computing: Automating the Virtualized Data Center*, Indianapolis: Cisco Systems, Inc., 2012.

[8] Public or Private Cloud (2013). *Aerohive NETWORKS*. Dostopno na: http://www.aerohive.com/pdfs/Aerohive-Whitepaper-Public-or-Private-Cloud.pdf.

[9] Virtulization (2014). *Wikipedia*. Dostopno na: https://commons.wikimedia.org/wiki/File:Hardware_Virtualization.JPG.

[10] Secure Virtualization for Cloud Environment Using Hypervisor-based Technology (februar, 2011). *International Journal of Machine Learning and Computing*. Dostopno na: http://www.ijmlc.org/papers/87-A888.pdf.

[11] (2014) Phishing Scams Lead to Identity Theft. Dostopno na: http://www.cccindy.com/credit-counseling-blog/phishing-scams-lead-to-identity-theft/.

[12] (2014) Switch. Dostopno na: http://www.techopedia.com/definition/2306/switch-networking.

[13] (2014) Network switch. Dostopno na: https://en.wikipedia.org/wiki/Network_switch.

[14] (2014) VSwitch. Dostopno na: http://www.webopedia.com/TERM/V/VSwitch.html.

[15] (2014) Virtual switch, definition. Dostopno na: http://www.techopedia.com/definition/27140/virtual-switch-vswitch.

[16] VMware Virtual Network concepts (julij, 2007). *VMware*. Dostopno na: https://www.vmware.com/files/pdf/virtual_networking_concepts.pdf.

[17] (2014) Informacijska varnost. Dostopno na: http://infosec.si/index.php?paged=2.

[18] Auditing Security Risks in Virtual IT Systems (2011). *ISACA*. Dostopno na: http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Documents/jpdf11v1-auditing-security-risks.pdf.

[19] Guidelines on Security and Privacy in Public Cloud Computing (januar, 2011). *NIST National Institute of Standards and Technology*. Dostopno na: https://downloads.cloudsecurityalliance.org/initiatives/guidance/NIST-Draft-SP-800-144_cloud-computing.pdf.

[20] Top Threats Working Group The Notorious Nine Cloud Computing Top Threats in 2013 (februar, 2013). *Cloud Security Alliance*. Dostopno na: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.