Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-642-645

BEZBEDNOSNI ASPEKTI VIRTUELIZACIJE

Vladimir Dobrosavljević, Dragan Polimac
Singidunum Univerzitet, Srbija

Abstract:
Virtuelizacija kao tehnologija je postala trend u svetu bez koga se teško može zamisliti rad Data centara modernih kompanija, samih kompanija i Cloud-a. Iako je virtuelizacija kao tehnologija dosta dugo prisutna, tek razvojem podrške za virtuelizaciju na x86 platformi postala je široko zastupljena, kako u velikim preduzećima, tako i kod manjih korisnika. Sa širenjem virtuelizacije postavlja se pitanje njene bezbednosti. Virtuelno okruženje je kompleksno tako da virtuelizacija u kolaboraciji sa mrežom kreira novu hibridnu mrežu koja zahteva nove bezbednosne mere. Ove mere uključuju tradicionalne mere bezbednosti kao i dodatne mere zbog same prirode virtuelizacije. U ovom radu su opisani bezbednosni aspekti virtuelizacije, propusti-ranjivosti, rizici koji su direktno vezani za samu tehnologiju i date su preporuke za unapređenje sistema bezbednosti.

Key words:
virtuelizacija; hipervizor; virtuelna mašina; vlan.

UVOD

Virtuelizacija je na mala vrata ušla u svet informacionih tehnologija. Iako sam koncept virtuelizacije seže 50 godina u prošlost, sama tehnologija se još uvek razvija, a posebno na polju servera i aplikacija. Polovina servera u celom svetu radi sa virtuelnim mašinama a na osnovu istraživanja IDC (International Data Corporation - USA), predviđa se da će s taj broj popeti do 70% do kraja 2014. godine. Da bi se održao korak sa tehnološkim napretkom i sve više rasprostranjenom implementacijom, mora se obratiti pažnja na bezbednost virtuelnih komponenti i samih virtuelizovanih okruženja.

BEZBEDNOSNI ASPEKTI TEHNOLOGIJE VIRTUELIZACIJE

Tehnologija virtuelizacije nam inicijalno omogućava neke bezbednosne aspekte, a to su:

1. Centralizovano skladištenje podataka koje sprečava gubitak podataka u slučaju krađe uređaja, gubitka uređaja i dr;
2. U slučaju izolovanosti virtuelne mašine od aplikacije, samo je jedna aplikacija na jednom operativnom sistemu podložna napadu;
3. Ukoliko je virtuelna mašina zaražena virusom, ona se može vratiti na pređašnje stanje, tj. stanje koje je bilo pre napada;
4. Smanjenje količine hardvera, samim tim i mogućnosti otkaza, samim tim i manje data centara;
5. Mogućnost iskorišćenja virtuelizacije desktopa za bolju kontrolu korisničkog okruženja. Administrator može napraviti i održavati „zlatnu kopiju“ koja se po potrebi distribuira korisnicima. Ova tehnologija nam omogućava bolju kontrolu operativnih sistema, što za posledicu ima direktno odgovaranje zahtevima kompanija kao i sigurnosnim polisama;
6. Virtuelizacija servera nam omogućava bolje upravljanje incidentima, s obzirom da servere možemo uvek vratiti u pređašnje stanje, odnosno stanje pre incidenta, da bi dijagnostifikovali šta se desilo pre i tokom incidenta;
7. Kontrola pristupa sistemskom i mrežnom delu infrastrukture, kao i delegiranje odgovornosti korisnicima se ogleda u tome, što se određenim korisnicima može dati pristup samo virtuelnim mašinama u okviru jedne mreže, dok se npr. drugoj grupi korisnika može dati kontrola virtuelnih mašina koje rade u DMZ. Još jedan od primera je da se određenoj grupi korisnika može dati pristup Windows serverima, dok druga grupa korisnika može pristupati isključivo Linux serverima.
8. Hipervizor je jednostavan i softver koji nije previše zahtevan, što direktno ima za posledicu manju marginu napada na sam hipervizor. Što je manja margina napada na hipervizor, to je manje potencijalnih sigurnosnih propusta;
9. Virtuelni svičevi ne rade dinamičko trunkovanje, što je uslov za *Inter-switch link tagging* napad. Oni odbacuju pakete sa duplom encapsulacijom tako da ta vrsta napada nije efektivna. Virtuelni svičevi ne

dozvoljavaju paketima da izađu iz svojih broadcast domena, tako da time onemogućavaju multicast brute force napad koji se oslanja na preopterećenje svičeva da bi se mogao izvršiti broadcast u druge VLAN domene.

Virtuelizaciona tehnologija je sama po sebi kompleksna, i da bi se iskoristili svi integrisani bezbednosni aspekti, sam sistem mora biti propisno konfigurisan.

BEZBEDNOSNI IZAZOVI, RIZICI I PROBLEMI SA VIRTUELIZACIJOM

Pored navedenih benefita, virtuelizacija nam donosi i neke izazove i rizike i to:

- *Deljenje fajlova između hostova i guest operativnih sistema*. Kada se koristi opcija deljenja fajlova, kompromitovani guest operativni sistem može da modifikuje ili promeni direktorijume koji se koriste za deljenje. Kada se koristi deljenje clipboard memorije i koristi se drag and drop, ili kad se koriste neki API za programiranje, pojedine rupe u ovim opcijama mogu kompromitovati kompletnu virtuelnu infrastrukturu;
- *Snapshots.* Kada se sistem vraća na predašnje stanje korišćenjem tehnologije *snapshot*-a, bilo koje promene napravljene u konfiguraciji se gube. Ako ste, na primer, promenili sigurnosnu polisu neki entiteti vam mogu postati nedostupni. Dnevnik aktivnosti (*audit log*) će se takođe izgubiti, što eleminiše dnevnik promena koje ste napravili na serveru. *Snapshot* fajlovi sadrže lične podatke kao što su lozinke, isto kao što se nalaze na fizičkom disku. Bilo kakav gubitak ili nenamerno kopiranje fajlova može predstavljati narušavanje bezbednosti. *Snapshot* fajlovi u sebi nekada mogu imati instaliran malware koji nije detektovan i pri sledećem pokretanju mogu narušiti bezbednost sistema;
- *Mrežno skladištenje podataka*. Fibre Channel i iSCSI predstavljaju clear text protokole i mogu biti ranjivi na *man-in-the-middle* napad. Alati za snimanje mrežnog saobraćaja se mogu iskoristiti za čitanje ili snimanje mrežnog-skladišnog saobraćaja a mogu se iskoristiti i za kasniju rekonstrukciju podataka od strane napadača. Takođe postoji bezbedna (*secure*) implementacija Fibre Channel protokola ali su performanse na niskom nivou, s obzirom da se enkripcija se koristi na host bus adapterima, što se direktno negativno odražava na performanse;
- *Hipervizor*. Ako je hipervizor kompromitovan, bilo koje virtuelne mašine koje se izvršavaju na tom hipervizoru će biti kompromitovane te je uvek preporučljivo promeniti inicijalnu konfiguraciju hipervizora. Hipervizor kontroliše sve i predstavlja *single-point-of-failure* u virtuelnom okruženju. Samo jedan bug može kompromitovati celu virtuelnu infrastrukturu. Bare metal hipervizori često sadrže kontrolu pristupa dok hipervizori koji je instaliraju na fizičkim serverima i njihovim operativnim sistemima (virtuelizacija na operativnom sistemu) ne sadrže takvu funkcionalnost. Virtuelizacija na operativnom sistemu je otvorenija na napade usled više pretnji koje direktno proističu iz operativnog sistema na kome se izvršava virtuelizacioni softver. Administrator na hipervizoru može da uradi sve („ima ključeve od kraljevstva"). Administratorska lozinka se može deliti između korisnika (više administratora), tako da se ne može znati šta je ko tačno uradio/izmenio na sistemu. Hipervizori mogu da dozvole virtuelnim mašinama međusobnu mrežnu komunikaciju i ova mrežna komunikacija neće izaći izvan okvira hipervizora. Navedena mreža se ponaša kao lokalna mreža za virtuelne mašine. Nad ovim mrežnim saobraćajem nije moguć nadzor i upravljanje jer se sav saobraćaj odvija unutar hipervizora, tako da ne može doći do kontrole onog što se fizički ne vidi;
- *Virtuelne mašine*. Virtuelne mašine su dovoljno male i veoma se lako kopiraju na neki udaljeni računar ili na neki prenosni disk. Gubitak podataka iz virtuelne mašine je jednak upadu u data centar prolazeći kroz fizičku zaštitu i otuđenje fizičkog servera. Virtuelne mašine koje instaliraju korisnici često ne ispunjavaju sve bezbednosne zahteve i nisu kompatibilne sa sigurnosnim polisama a i veoma često nemaju instaliran sigurnosni softver. Virtuelne mašine se tipično kreiraju sa svim otvorenim portovima i mnogim nepotrebnim protokolima. Svaki put kada se instalira nova virtuelna mašina, još jedan operativni sistem je dodat, koji treba biti zaštićen, pečovan, osvežavan i održavan. Svaki novi operativni sistem utiče na kompletnu bezbednost virtuelnog sistema. Neaktivne virtuelne mašine ili virtuelne mašine koje se više ne koriste (skrivene virtuelne mašine) mogu da sadrže važne podatke kao što su *user credentials* i konfiguracije. Svaka funkcionalnost za deljenje clipboard-a između virtuelnih mašina mogu predstavljati vrata za malware aplikacije. Virtuelne mašine koje nisu izolovane imaju pun pristup resursima hosta, te bilo kakvo kompromitovanje virtuelnih mašina vodi do kompromitovanja svih resursa. Virtuelne mašine mogu biti kreirane od strane korisnika koji nemaju ekspertska znanja na polju IT, i kao takve neće biti zaštićene. Inficiranje virtuelne mašine može dovesti do inficiranja skladišta podataka i druge virtuelne mašine mogu koristiti to isto skladište podataka tako da time mogu kompromitovati svoj dalji rad. Virtuelne mašine brzo rastu i taj rast je praćen povećanjem sigurnosnih pretnji. Ako nisu efektivno automatizovane, administrator će imati dodatnog posla pri održavanju, osvežavanju, krpljenju... Zaražene virtuelne mašine se mogu pojaviti u sistemu, zatim zaraziti druge računare i nestati bez traga;
- *Delegacija odgovornosti i administrativni pristup*. U tipičnim fizičkim mrežama, server administratori upravljaju serverima, dok mrežni administratori upravljaju samo mrežom. Security osoblje obično sarađuje i sa server i sa mrežnim administratorima. U virtuelizovanom okruženju, upravljanje serveri-

ma i mrežom se može nalaziti na istoj upravljačkoj konzoli i ovo predstavlja izazov, kako efektivno delegirati odgovornosti i administraciju. Inicijalno, mnogi sistemi za virtuelizaciju dodeljuju pun pristup svim aktivnostima u virtuelnom okruženju. Ova inicijalna podešavanja se često ne menjaju i kompromitovanje ovih podešavanja i administratorskog pristupa sistemu dovodi do pune kontrole nad virtuelnom infrastrukturom;

- *Sinhronizacija vremena*. Vreme na virtuelnim mašinama može biti promenjivo i kasniti i u kombinaciji sa normalnim kašnjenjem, zadaci se mogu izvršavati ranije ili kasnije što direktno ima za posledicu gubitak tačnosti rada sistema. Netačno vreme nam neće omogućiti preciznu dijagnostiku i digitalnu forenziku pri nekim budućim analizama;
- *Virtual LAN (VLAN)*. Korišćenje VLAN-ova zahteva rutiranje saobraćaja virtuelne mašine od hosta ka firewall-u. Ovo može dovesti do kašnjenja i kompleksne mrežne arhitekture, što direktno utiče na performanse. Saobraćaj između VLAN-ova ne podleže nadzoru i nije zaštićen. Takođe, ako je više virtuelnih mašina u istom VLAN-u znatno je olakšano širenje malware aplikacija;
- *Deljenje resursa*. Pretpostavka je da pri izvršavanju više virtuelnih mašina na hostu, svaka od njih je izolovana i ne može biti iskorišćena u svrhu napada na druge virtuelne mašine. Tehnički virtuelne mašine su razdvojene, ali sve virtuelne mašine dele zajedničke resurse kao što su: CPU, memorija i mrežni protok. Ako jedna mašina zauzme veliki deo nekog resursa, npr. zbog nekog virusa, denial-of-service napad se može manifestovati na drugim resursima;
- *Ostali problemi*. U današnje vreme bezbednosne polise se najčešće nalaze u „glavama" administratora ili u tzv. *check lists* listama, i zbog same prirode virtuelnog okruženja i njegove brze promene, teško je ispratiti sve sigurnosne polise. Virtuelizacija se u osnovi bazira na softveru, što direktno reflektuje ranjivost softvera i margina napada se povećava. Virtuelni diskovi obično ne sadrže enkriptovane podatke, tako da kompromitovanje ovih podataka je jednako tome da imate otvoren pristup svim resursima. Virtuelne mašine različitih nivoa bezbednosti (sigurnosti) se mogu istovremeno izvršavati na jednom serveru i koristiti jedan virtuelni svič i bezbednost tog hosta tj. virtuelnog sviča direktno zavisi od „najslabije karike" tj. virtuelne mašine sa najmanjim nivoom bezbednosti.

Uprkos tome što smo identifikovali veliki broj potencijalnih bezbednosnih propusta, sama tehnologija virtuelizacije nije obavezno nesigurna, međutim, način na koji je implementirana može sama po sebi biti nebezbedne prirode. Nepotpune bezbednosne politike i procedure, kao i nedovoljna obučenost administratora, može biti veći uzrok problema i ranjivosti koje mogu dovesti do još većeg rizika po sam sistem. Pošto su opisani bezbednosni aspekti vezani za virtuelizaciju, navešćemo neke od uobičajenih napada.

NAJČEŠĆE VRSTE NAPADA U VIRTUELNOM OKRUŽENJU

Najčešće vrste napada koje se sreću u virtuelnom okruženju predstavljaju:

- *Denial of Service (DoS)*. Uspešan DoS napad može dovesti do nasilnog gašenja/isključenja hipervizora. Ovo može dovesti do ranjivosti u sistemu, koja omogućuje skrivena vrata i pristup virtuelnim mašinama koje se izvršavaju na tom hipervizoru.
- *Skakanje između virtuelnih mašina (VM jumping)*. Ako postoji bezbednosni propust u hipervizoru i taj propust bude iskorišćen za pristup nekoj virtuelnoj mašini, maliciozni korisnik može skakati sa jedne virtuelne mašine na drugu i pristupiti svim podacima.
- *Praćenje sistemskog saobraćaja hosta (Host Traffic Interception)*. Bezbednosni propusti u hipervizoru mogu da dozvole praćenje sistemskih poziva, page fajlova i praćenje aktivnosti memorije i diskova.
- *Virtuelni maliciozni kod*. Bezbednosni propust koji dozvoljava napadaču da kreira novu virtuelnu mašinu sa ograničenim privilegijama, na kojoj se instalira maliciozni kod. Maliciozni kod se povezuje na postojeće virtuelne mašine i kreira novi virtuelni emulator, u kome pokreće slike virtuelnih mašina koje je uspeo da poveže.
- *VM sprawl*. Virtuelne mašine se vrlo lako kreiraju, čak je u *Cloud*-u to potpuno automatizovan proces. Napadač može iskoristiti rootkit alate i da zauzme sve resurse na hostu.
- *Nebezbedna izolacija virtuelnih mašina*. Izolacija hosta predstavlja sigurnosni mehanizam za osiguravanje visoke dostupnosti i kontinuiteta rada aplikacija i servisa u virtuelnoj infrastrukturi. Napadač to može iskoristiti i povezati virtuelne mašine na sopstvenu mrežu i time dobiti pristup svim resursima.
- *Nebezbedna migracija virtuelnih mašina*. Često se virtuelne mašine migiriraju na nove hostove koji se nalaze u delovima virutelne infrastrukture, na kojima nisu implementirani svi bezbednosni mehanizmi i primenjene sve preporuke za povećanje bezbednosti.

Postoji još puno vrsta napada koje se mogu iskoristiti u virtuelnom okruženju i te vrste napada su konkretno vezane za pojedine komponente virtuelnog okruženja na koje se virtuelno okruženje oslanja (svičevi, ruteri, serveri i druge vrste uređaja).

PREPORUKE ZA POVEĆANJE BEZBEDNOSTI

Inženjeri bezbednosti moraju postaviti smernice za smanjenje bezbednosnih rizika. Prvi zadatak koji im se postavlja je da precizno definišu osobine i kapacitet virtuelne infrastrukture i da aktivno prate stanje hipervizora i samih virtuelnih mašina. Kao dodatno treba se obatiti pažnja i na:

- *Monitoring saobraćaja između virtuelnih mašina*. Sposobnost praćenja *backbone* saobraćaja virtu-

elnih mašina je najbitnija stavka. Tradicionalni softveri za praćenje saobraćaja ne mogu pratiti saobraćaj na softverski definisanim virtuelnim svičevima, međutim sam hipervizor nam omogućava da pratimo saobraćaj i uvek se treba obratiti pažnja na te mogućnosti.

- *Administrativna kontrola.* Često može doći do kompromitovanja *user credentials*-a za upavljanje virtuelnom infrastrukturom na veliki broj načina (rootkit, socijalni inženjering, keylogger...) tako da treba obezbediti procedure za autentifikaciju, upravljanje identitetima (*identity management*) i snimanje aktivnosti (*logging*).
- *Customer Security.* Lica koja pristupaju servisima dolaze u direktan kontakt sa interfejsom servisa, moraju imati implementirane zaštitne mehanizme.
- *Segmentacija virtuelnih mašina.* Kao dodatak izolaciji hostova, poželjno je i funkcionalno razdvojiti virtuelne mašine. Na primer, poželjno je razdvojiti bezbednosne zone u kojima se nalaze vituelni serveri i virtuelne desktop mašine. Cilj je da se minimizira broj spojnih tačaka u meri u kojoj je to moguće.

ZAKLJUČAK

Virtuelizacija nam donosi nove bezbednosne izazove sa kojima se moramo suočavati. Virtuelne komponente i virtuelno okruženje ne može biti zaštićeno postojećim bezbednosnim mehanizmima i bezbednosnim procedurama.

Virtuelizacija kreira hibridnu mrežu između fizičke mreže i nove virtuelne ili logičke mreže. Da bi se postigao visok nivo bezbednosti virtuelnog okruženja, dodatni napori i mere zaštite se moraju implementirati, što se direktno odražava na proces planiranja i implementacije, obuke korisnika, koji mora biti unapred dobro i kvalitetno pripremljen i urađen.

Bezbednost virtuelne infrastrukture ne sme biti ideja koja se javlja nakon implementacije virtuelne infrastrukture i svih njenih komponenti.

Bezbednosni aspekti na polju virtuelizacije će u budućnosti napredovati kako i sama tehnologija virtuelizacije napreduje, a kao sledeći korak očekuje se uvođenje standarda koji se moraju ispoštovati, da bi se obezbedilo svako novo virtuelno okruženje.

LITERATURA

[1] Amy Larsen DeCarlo, "Myth vs. Reality: Controlling VM Sprawl in the Cloud", http://searchcloudprovider.techtarget.com/tip/myth-vs-reality-controlling-vm-sprawl-in-the-cloud

[2] Virtualization Security Fundamentals, http://www.sans.org/course/virtualization-security-fundamentals

[3] Security Implications of the Virtualized DataCenter http://www.f5.com/pdf/white-papers/virtual-data-center-security-wp.pdf

[4] Trend Micro, „Meeting the Challenges of Virtualization Security", http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_meeting-the-challenges-of-virtualization-security.pdf

[5] Haletky, Edward L., „Contributor. Securing Virtual Environments: Three Considerations" , http://secureserver-virtualization.techtarget.com/tip/securing-virtual-environments-three-considerations

[6] Lowe Scott, "How iSCSI Packets Are Encapsulatedand How to Protect

[7] iSCSI Data Traffic" http://www.techrepublic.com/blog/networking/how-iscsi-packets-are-encapsulated-and-how-to-protect-iscsi-data-traffic/5398

[8] Common Virtualization Vulnerabilities and How to Mitigate Risks, http://pentestlab.wordpress.com/2013/02/25/common-virtualization-vulnerabilities-and-how-to-mitigate-risks/

VIRTUALIZATION SECURITY

Abstract:
Virtualization as a tehnology has become a growing trend in the world, without which one can not imagine the work od the modern data centers, companies and Cloud. Although it is a virtualization technology for a long time hovering around the development of support for virtualization on the x86 platform has become widely represented in both large enterprises and smaller users in person. With virtualization growth the security issue pops up. The bottom line, new virtual environment is complex and virtualization together with network establishes a new hybrid network which demands new security methods. This methods include traditional security methods as well as additional measures which derive from the virtualization itself. This paper describes virtualization security aspects, problems and risks that are directly attached to the virtualization technology and recommendations for increasing security are given.

Key words:
virtualization,
hipervisor,
virtual machine,
vlan.