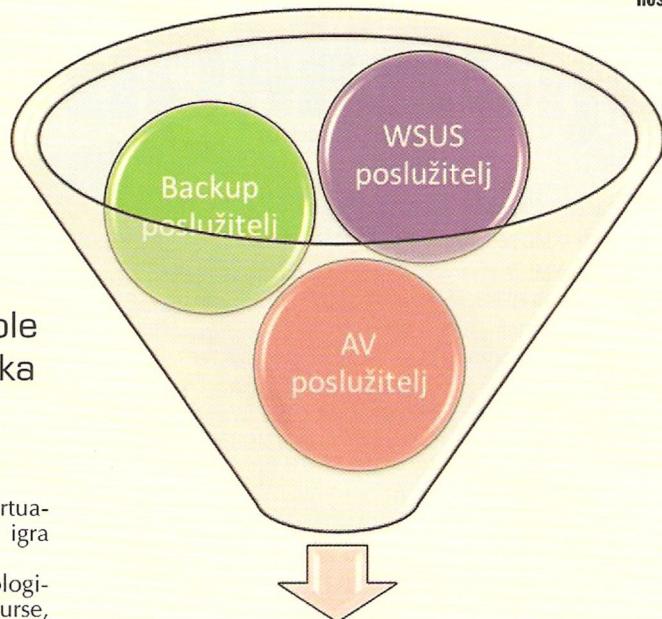


Rizici virtualnih okruženja

Konsolidacija više fizičkih poslužitelja u virtualne koji će se izvoditi na hostu



Uspostavili ste virtualno okruženje i konsolidirali desetke poslužitelja u virtualne koji se vrte na šačici fizičkih poslužitelja.

Primjenili ste standardne sigurnosne kontrole kao i uvijek do tada. Jeste li svjesni novih rizika koje ste uveli u svoj informacijski sustav?

DALIBOR UREMOVIĆ

Virtualizacija IT sustava, iako tek relativno odnedavno u masovnoj upotrebi, datira još iz 70-ih godina, kada je IBM uveo virtualizacijsku tehnologiju u svoje mainframe sustave. Nažalost, ovi masivni sustavi bili su (i jesu) veliki potrošači energije, kao i današnji fizički poslužitelji koji često ne iskoriste svoj puni kapacitet. Posljednja istraživanja pokazuju kako voditelji IT organizacijskih jedinica sve češće govore o uštedama u struji i prostoru, uglavnom se pozivajući na pojam

zeleni IT (*green IT*). Virtualizacija u ovom slučaju igra značajnu ulogu.

Virtualizacija je tehnologija koja dijeli fizičke resurse, poput poslužitelja, u virtualne resurse zvane virtualne mašine. Pritom jedan fizički poslužitelj na sebi sadrži više virtualnih mašina, odnosno logičkih poslužitelja. Ovu konsolidaciju logičkih poslužitelja na jedan fizički nazivamo virtualizacijom. Virtualizacija pomaže da se smanji broj fizičkih poslužitelja, pojednostavi administracija, smanji

potrošnja električne energije, energije za hlađenje i sl.

Premda je virtualizacija poslužitelja najčešći korišteni oblik ove tehnologije, ona nije ograničena samo na poslužitelje. Moguće ju je primijeniti i na razini operacijskog sustava, radnih površina (desktopa), aplikacija, mreže i sl. Primjerice, kod virtualizacije sustava za pohranu podataka fizički se sustav od nekoliko uređaja prikazuje kao jedan logički uređaj za pohranu.

Arhitektura virtualizacijske tehnologije

Virtualni poslužitelji dovode do toga da se više instanci operacijskih sustava i aplikacija pokreće na istom fizičkom uređaju. One se izvode u izoliranim okruženjima (virtualne mašine), a za njihovo se koordiniranje brine virtualizacijski sloj zvan hipervizorom. On je zadužen za predstavljanje fizičkih resursa poput procesora, memorije, mrežnih resursa i sl. virtualnim mašinama kako bi ih one znale koristiti. Neke od tehnologija kojima je realiziran hipervizor jesu Microsoft Hyper-V, VMware ESX, Citrix XenServer itd. Glavne komponente virtualizacijske tehnologije opisane su u okviru sa strane.

Virtualne mašine mogu izvoditi različite aplikacije na različitim operacijskim sustavima, a na hostu se nalaze u obliku jedne ili više datoteka na datotečnom sustavu. Zbog toga ih je jednostavno kopirati, premještati i raditi rezervne kopije. Virtualne su mašine potpuno izolirane jedna od druge i u idealnom slučaju pad jedne ne

Virtualne mašine	<ul style="list-style-type: none"> Razni poslužitelji informacijskog sustava koji su virtualizirani
Virtualizacijski softver (eng. hypervisor)	<ul style="list-style-type: none"> Softver koji koordinira resurse host poslužitelja s zahtjevima virtualnih mašina (npr. snaga procesora, raspoloživa memorija, disk, propusnost mreže i sl.)
Operativni sustav host poslužitelja	<ul style="list-style-type: none"> Primarni OS na fizičkom poslužitelju. Virtualizacijski softver je instaliran na ovom OS-u
Fizička oprema (hardver)	<ul style="list-style-type: none"> Fizički poslužitelj(i) na kojem je postavljeno virtualno okruženje; Mrežni uređaji kojima su realizirane veze host poslužitelja (i posredno virtualnih mašina) s ostatkom sustava; Sustav za pohranu podataka (eng. storage)

Vrijednost imovine	Razina prijetnje									
	Mala			Srednja			Velika			
	Razina ranjivosti									
	M	S	V	M	S	V	M	S	V	
0	0	1	2	1	2	3	2	3	4	
1	1	2	3	2	3	4	3	4	5	
2	2	3	4	3	4	5	4	5	6	
3	3	4	5	4	5	6	5	6	7	
4	4	5	6	5	6	7	6	7	8	

Vjerljost ostvarivanja prijetnje	Utjecaj				
	Vrlo veliki (100)	Umjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)	
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)	
Umjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)	
Srednja do mala (0,3)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)	
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)	

a) Imovina * Prijetnja * Ranjivost

b) Vjerljost ostvarivanja prijetnje * Utjecaj na imovinu

Izračun visine rizika - dva najčešća načina

uzrokuje pad druge virtualne mašine ili hosta.

Sa sigurnosnog stajališta, neke su od prednosti virtualizacije: sigurnije i brže upravljanje zakrpama, lakša kontrola i administracija, brži oporavak nakon sigurnosnog napada, lakša forenzička analiza i sl.

Rizici virtualnih okruženja

Naravno da nije sve tako bijelo. Kao i svaka druga, tako je i virtualizacijska tehnologija donijela neke nove uz pregršt starih IT rizika. Štoviše, prema jednoj Gartnerovoj studiji iz 2010. godine, u ovoj će godini gotovo polovina poslužitelja biti virtualna, a 60% virtualnih mašina biti manje sigurno nego bi to bili njihovi fizički pandani. Stoga je važno redovito raditi procjene rizika ove tehnologije u okruženjima tvrtki kako se ova pogubna prognoza ne bi ostvarila.

Prvu grupu rizika čine rizici zbog arhitekturnih ranjivosti. Kao što je virtualna

mašina podložna istim napadima kao i host (potencijalnom se napadaču svi poslužitelji predstavljaju kao posebni resursi sa svojim IP adresama i sl.), sigurnosne kontrole poput antivirusnih klijenata, ojačanja OS-a, analiza servisa, portova i sl. moraju se provesti na svim mašinama. Na sve mašine redovito se moraju primjenjivati zatrpe, a segregacija mreže odnosno mrežnog prometa mora se napraviti kako da se radi o više različitih fizičkih poslužitelja.

Drugu grupu rizika čine rizici zbog softverskih ranjivosti. Uvjeto rečeno, najvažnija je softverska komponenta hipervizor. Bilo kakva ranjivost u ovoj komponenti automatski predstavlja i rizik za sve virtualne mašine. Kako bi se ovi rizici smanjili, potrebno je primijeniti sljedeće kontrole: redovito ažuriranje hipervizora najnovijim zakrpama proizvođača, strogu kontrolu pristupa na host odnosno konzolu hipervizora, ojačanje operacijskog sustava hosta kako bi se smanjila mogućnost zločudnih

napada te organizacijske procedure za administraciju, odnosno upravljanje pojedinih virtualnih mašinama.

Na kraju možemo govoriti i o konfiguracijskim rizicima. Kako je vrlo lako moguće novu infrastrukturu virtualizirati (tzv. *physical to virtual* tehnika potpomognuta softverom), kontrola i administracija ovih novih brzo instaliranih virtualnih mašina postaje kritični problem. Upravljanje ovim rizicima lakše je uz formalno uspostavljanje procesa upravljanja promjenama i konfiguracijama koje je inače teško implementirati - ako ni zbog čega drugog, onda zbog velikog broja različitih tipova resursa i tipova promjena odnosno zapisa koje je potrebno voditi. Osim ovih procesa, valja voditi redovite revizije konfiguracija hipervizora i virtualnih mašina te instalirati samo odobrene predloške virtualnih mašina (npr. s već ojačanim konfiguracijama). Kako bi se smanjili rizici između pojedinih revizija, ne bi bilo loše implementirati i detaljni nadzor zapisa, odnosno dogadaja (*event monitoring*).

IT procesi i virtualizacija

Prilikom identifikacije ranjivosti informacijskog sustava i implementiranih postojećih kontrola vezanih uz virtualna okruženja dobro je voditi se metodologijom revizije informacijskog sustava. Revizija informacijskog sustava, bez obzira na to je li rađena s vlastitim djelatnicima ili uz pomoć vanjskih stručnjaka, uvijek se temelji na prosudbi kvalitete dizajna kontrola (*control design testing*), odnosno učinkovitosti implementiranih kontrola (*control efficiency testing*). Kontrole koje je potrebno testirati proizlaze implementacijom tipičnih IT procesa koji su propisani raznim svjetskim standardima i smjernicama, poput CobIT-a, ITIL-a i sl.

Procjenitelj rizika virtualizacije postaje, dakle, u koracima identifikacije ranjivosti i kontrola revizorom te testira dizajn i učinkovitost kontrola ➔

METODOLOGIJA PROCJENE RIZIKA

Danas je dostupno više svjetski poznatih metodologija za procjenu rizika. Neke su od poznatijih: NIST 800-30, Octave, Grundschatz, ISO 27005:2008, BS 7799:3-2006, Mehari. Ma koju odabrali, svima su koraci vrlo slični i mogu se ugradno nabrojiti kako slijedi: karakterizacija okruženja, identifikacija prijetnji, identifikacija ranjivosti odnosno analiza implementiranih sigurnosnih kontrola, izračun visine rizika prema odabranoj metodi, dokumentiranje rezultata. Karakterizacijom okruženja upoznat ćemo se s opsegom virtualnog okruženja te

popisati komponente sustava, veze između njih te korištene tehnologije, o čemu govoriti prvi dio ovog članka. Ključan je korak identificirati prijetnje i ranjivosti, odnosno sustav već implementiranih kontrola. Pitanja navedena u posebnom okviru uz tekst mogu nam pomoći pri toj identifikaciji, a ove su aktivnosti niže još ponešto detaljizirane. Naravno, čim je veći i detaljniji set pitanja, uz ekspertizu onog tko radi procjenu rizika, dobit će se i kvalitetniji popis prijetnji, ranjivosti i kontrola. Zadnji je korak matematička kalkulacija visine rizika prema procijenjenim parametrima. Najčešći su parametri koji se pritom koriste

vjerljost da prijetnja iskoristi ranjivost te utjecaj na poslovanje ako se to dogodi. Neke metodologije koriste i vrijednosti (uvjetno rečeno) promatrane informacijske imovine, prijetnje i ranjivosti, čiji umnožak daje visinu rizika. Procjena rizika virtualnog okruženja, koristeći metodološki pristup te ekspertizu procjenitelja, daje nam mogućnost da se fokusiramo na kritične propuste postavljenog sustava te sveobuhvatno analiziramo sigurnost virtualnog okruženja sa stanovišta povjerenljivosti, cjelevitosti i povjerenljivosti informacija koje se njime obrađuju.

Procjena rizika informacijskih sustava

standardnih IT procesa, a može se (i preporučljivo je) voditi već gotovim izvještajima službenih revizora informacijskih sustava. Jedan od važnijih IT procesa odnosi se na upravljanje promjenama u informacijskom sustavu, u sklopu kojeg procjenitelj provjera aktivnosti kreiranja, instaliranja i konfiguriranja virtualnih mašina. Drugi je važan proces nadzor korištenja sustava. Ovdje je posebno interesantan status virtualnih mašina - radi, ne radi, suspendirana/onemogućena. I dok se za virtualne mašine u statusu "radi" prepostavlja određena razina upravljanja sigurnošću, ugašene odnosno suspendirane mašine često su pune sigurnosnih rupa te predstavljaju značajan sigurnosni rizik prilikom pokretanja. Proces upravljanja konfiguracijama informacijskog sustava također je u fokusu provjere zbog već prije navedenih inherentnih rizika (lakoća kreiranja i kopiranja virtualnih mašina dovodi do čestih izmjena postojeće konfiguracije informacijskog sustava, a koje pritom ostanu neprovjere).

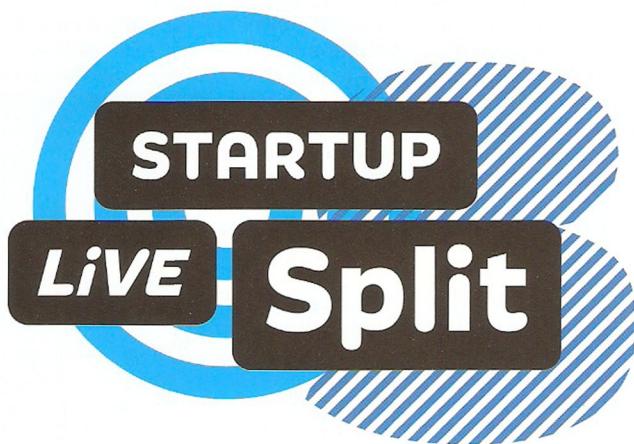
Kako se procjena rizika ne bi oslonila samo na generičke prijetnje i ranjivosti koje proizlaze iz dodirnih IT procesa te kontrola koje se odnose na bilo koju tehnologiju kojom je realizirano virtualno okruženje, bitno je identificirati i one specifične prijetnje, ranjivosti i kontrole korištene virtualizacijske tehnologije.

Neka od pitanja procjene rizika virtualnih okruženja

1. Postoji li dovoljno stručnih znanja u IT-u tvrtke za upravljanje virtualnim okruženjem?
2. Postoji li i gdje se nalazi jedinstvena točka prekida poslovanja (*single point of failure*)?
3. Jesu li identificirani sigurnosni zahtjevi virtualnog okruženja?
4. Tko ima pravo administracije na hostu?
5. Prate li se sistemski zapisi pristupa hostu?
6. Mogu li administratori hosta pristupiti tim sistemskim zapisima i mijenjati ih ili brisati?
7. Koristi li se host za druge svrhe osim za upravljanje virtualnim okruženjem?
8. Koje kontrole postoje vezane uz kopiranje virtualnih mašina?
9. Postoji li podjela virtualnog okruženja na zone prema osjetljivosti virtualnih mašina, odnosno prema informacijama koje se nalaze na pojedinim virtualnim mašinama?
10. Postoje li propisane procedure, odnosno upute za rad s virtualnim okruženjem?
11. Postoji li jasna i dokumentirana procedura s listom za provjeru aktivnosti pri instaliranju nove virtualne mašine?
12. Je li provedeno sigurnosno ojačanje (*hardening*) virtualnih mašina?
13. Je li provedeno sigurnosno ojačanje (*hardening*) hosta?
14. Radi li se pričuvna pohrana virtualnih mašina prema zahtjevima poslovanja?
15. Tko ima pravo na pristup pričuvnoj pohrani?
16. Primjenjuju li se redovito najnovije sigurnosne zakrpe na virtualnim mašinama i hostu?
17. Jesu li kontrole fizičkog pristupa do hosta u skladu s najkritičnjom virtualnom mašinom?
18. Izvršava li se na hostu bilo kakav servis dostupan putem mreže?
19. Postoji li mogućnost da jedna od virtualnih mašina zauzeće velikog dijela resursa ugrozi rad ostalih?
20. Postoje li nepotrebne (*disabled*), testne i razne probne virtualne mašine u katalogu na hostu?

Svi vodeći igrači na ovom polju, poput VMwarea, Microsoft Hyper-V-a ili Citrix Xena, već imaju izdane svoje smjernice i tehničke standarde za ojačanje sigurnosti

virtualnih okruženja koje je samo potrebno primijeniti, kako pri implementaciji, tako i kod revizije odnosno procjene rizika virtualizacije.



Powered by
procedo

Sponsori

HRVATSKI
NEZAVISNI
IZVOZNICI SOFTVERA

si speedinvest

Info: www.procedo.hr/startuplivesplit

Kontakt: procedo@procedo.hr; tel: +385 21 352 478

PREDSTAVITE SVIJETU SVOJE IDEJE

procedo™