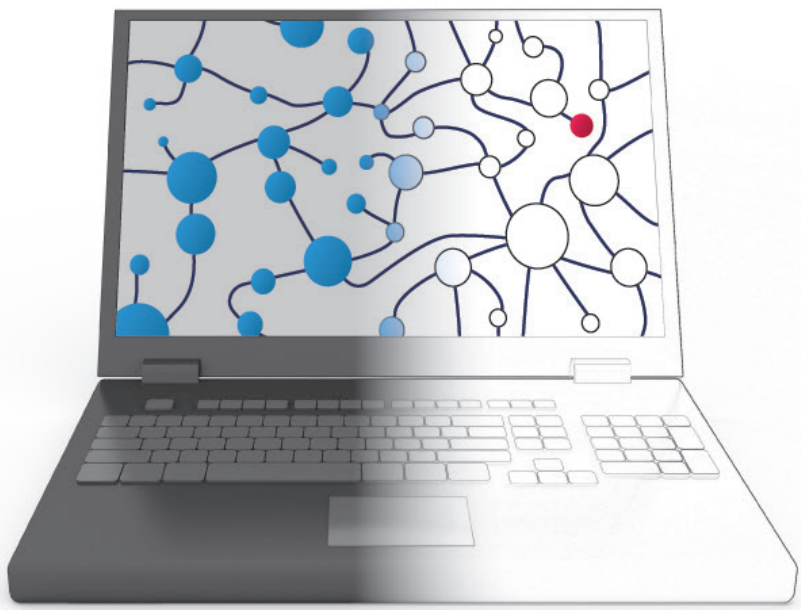
Risker med virtualisering av IT-system

DANIEL EIDENSKOG, MARTIN KARRESAND



FOI-R--4448--SE
ISSN 1650-1942 Juli 2017

FOI-R--4448--SE

Daniel Eidenskog, Martin Karresand

Risker med virtualisering av IT-system

Bild/cover: Daniel Eidenskog

Titel	Risker med virtualisering av IT-system
Title	Risks When Using Virtualization of IT Systems
Rapportnummer	FOI-R--4448--SE
Månad	Juli
Utgivningsår	2017
Antal sidor	46
ISSN	ISSN-1650-1942
Uppdragsgivare	Försvarsmakten
Projektnummer	E72677
Godkänd av	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Forskningsområde	Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI

Sammanfattning

Virtualisering av IT-system är en beprövad och utbredd teknik för att bygga såväl stora datacenterlösningar som mindre installationer. Virtualisering ger ett antal fördelar för drift och verksamhet, men innebär även risker. Denna rapport diskuterar virtualisering av IT-system med fokus på de risker och sårbarheter som kan uppstå i virtualiserade miljöer. Rapporten tar främst upp så kallad *systemvirtualisering*, det vill säga system där den virtualiserade miljön motsvarar en fysisk dator.

Studien baseras på en litteraturstudie av översikter avseende sårbarheter i virtualiseringsmjukvara. Målet med studien är att bidra till förståelsen för de risker som virtualisering innebär, genom att beskriva sårbarheter i etablerade virtualiseringsmjukvaror.

Virtualiserade miljöer innehåller i regel samtliga sårbarheter som finns i motsvarande fysiska miljöer. Virtualisering innebär dessutom att mjukvara tillförs i systemet för att skapa virtualiseringsmiljön, upprätthålla separation och ge ett lämpligt ”hårdvarulikt” gränssnitt mot de virtuella maskinerna. Den tillförda mjukvaran kan innehålla sårbarheter vilket ger ytterligare möjligheter för angripare. Jämfört med fysisk separation finns exempelvis ökad risk för läckage mellan virtuella maskiner och att virtuella maskiner påverkar varandra på oönskade sätt.

Risken för att lyckade angrepp ska få mer utbredda konsekvenser är i regel större i virtualiserade miljöer än i miljöer byggda på fysiskt åtskilda maskiner. I vissa fall är risken acceptabel utifrån de fördelar som virtualiseringen innebär. I andra fall, till exempel om separationen måste skydda information med hög informationssäkerhetsklass, så är risken hög med dagens virtualiseringstekniker. Införandet av virtualisering i ett kritiskt IT-system måste därmed föregås av noggranna riskbedömningar för att säkerställa att lämplig risknivå upprätthålls.

Nyckelord

Pålitliga IT-system, virtualisering, virtuell maskin, IT-säkerhetsrisk, sårbarhet

Abstract

Virtualization of IT systems is a mature and wide-spread technology, used for large data centers as well as smaller systems. Virtualization provides several advantages for operations, but also incurs risks. This report gives an overview of virtualization, focusing on risks and vulnerabilites that may arise in virtualized environments. This report mainly covers so called *system virtualization*, where the virtual environment corresponds to a physical computer.

The study is based on a literature study, collecting surveys on vulnerabilities in virtualization software. The objective of the study is to present vulnearabilites that have been reported in well-used virtualization software, with the intent to give an understanding of the risks brought by virtualization technology.

Virtualized environments typically include all vulnerabilities that are present in the corresponding physical environments. Virtualization also adds software to the system in order to create the virtualized environment, uphold the separation between virtual machines, and present a suitable ”hardware-like” interface to the virtual machines. The added software may contain vulnerabilities, which provide further attack surfaces. Examples of added risks when using virtualization include possible information leakage between virtual machines and that virtual machines may affect each other in undesirable ways.

The risk that an attack renders more widespread consequences in a virtual environment is generally higher compared to systems built using physically separated machines. The risk may be acceptable in certain cases, considering the advantages provided by virtualization. In other cases, for example where the separation protects highly classified information, the risk is too high with today’s virtualization techniques. Careful risk assesment is essential to ensure a suitable risk level when using virtualization.

Keywords

Trustworthy IT systems, virtualization, virtual machine, IT security risk, vulnerability

Innehåll

1 Inledning

Virtualisering innebär att en virtuell representation av någonting skapas. Inom IT-branchen innebär virtualisering i regel skapandet av en avgränsad miljö, som implementeras av mjukvara, i vilken en annan mjukvara kan köras med begränsat beroende till det underliggande fysiska systemet. Virtualisering kan användas på flera olika nivåer där det till exempel kan ge möjlighet att köra plattformsoberoende mjukvara såsom Java-bytekod eller för att frikoppla operativsystem från underliggande hårdvara.

Virtualisering av IT-system kan innebära förenkling av drift och förbättra för verksamheten, genom till exempel funktioner för lastbalansering mellan virtuella servrar och att förenkla utbyte av trasig hårdvara. Virtualisering innebär även risker, till exempel att det sker läckage av information mellan virtuella maskiner, att komplexa beroenden mellan olika funktioner kan ge svåröverskådliga effekter när dessa aktiveras och att det tillkommer ytterligare mjukvara som kan innehålla brister.

Denna rapport fokuserar på systemvirtualisering, det vill säga system där den virtualiserade miljön motsvarar fysiska datorer. Systemvirtualisering är ett återkommande ämne när arkitekturen för nya IT-system diskuteras inom Försvarsmakten. Det är lätt att förstå varför virtualisering är ett attraktivt alternativ då det ofta för med sig ett flertal positiva effekter i såväl verksamhet som drift. En stor del av dessa positiva effekter framhålls ofta i marknadsföringen från de som utvecklar och säljer virtualiseringslösningar, vilket innebär att de är relativt välkända. Det som saknas i debatten är konkreta översikter av de risker och de attackytor som virtualiseringen innebär. Inom Försvarsmakten är det vanligt att IT-system hanterar skyddsvärd information, i vissa fall med mycket högt skyddsvärde, vilket ställer stora krav på säkerhetsnivån i IT-miljön.

1.1 Syfte och mål

Syftet med studien är att presentera risker och angreppsytor som virtualisering av IT-system medför. Fokus i studien är de risker och angreppsytor som tillkommer vid virtualisering av servermiljöer.

Målet med studien är att svara på följande frågeställningar för virtualiserade IT-system:

- Vilka tekniska och administrativa risker tillkommer?
- Vilka angreppsvägar finns i virtualiserade system?
- Vilken övergripande effekt ger användade av virtualiseringsteknik på IT-säkerheten?
- Vilka huvudsakliga risker måste hanteras om virtualiseringsteknik ska användas för system med högt skyddsvärde?

I studien beaktas enbart virtualiseringssystem som är etablerade och därmed används i skarp drift. Denna avgräsning utesluter virtualiseringsmjukvaror som exempelvis utgörs av forskningsresultat och prototyper. Denna avgränsning syftar till att fokusera studien på sårbarheter och angrepp som kan förekomma i verkliga system.

1.2 Terminologi

Följande termer används i denna rapport:

- **Gäst** (eng. *guest*)
  Den mjukvara som körs i en virtualiserad miljö. I den här rapporten utgörs en gäst av ett operativsystem med underliggande applikationer om inget annat anges.
- **Hypervisor**
  Virtualiseringslagret i systemvirtualisering.
- **Systemvirtualisering** (eng. *system virtualization*)
  Virtualisering där den virtuella miljön motsvarar fysiska datorer.
- **Typ 1 (Native)**
  Systemvirtualisering där hypervisor kör direkt på hårdvaran.
- **Typ 2 (Hosted)**
  Systemvirtualisering där ett värdoperativsystem körs på hårdvaran och där virtualiseringsmjukvaran körs i värdoperativsystemet.
- **Virtualisering**
  Samlingsnamn för olika tekniker att skapa virtuella miljöer för mjukvara för att frikoppla denna från det underliggande systemet. I rapporten används termen synonymt med ”systemvirtualisering” förutom i detta kapitel.
- **Virtual Machine Monitor (VMM)**
  Annan term för hypervisor.
- **Värd** (eng. *host*)
  Den mjukvara som körs för att hantera den virtualiserade miljön. Värden kan exempelvis utgöras av ett operativsystem som körs i en priviligerad virtuell maskin eller av det operativsystem där den virtuella miljön körs.

1.3 Säkerhetsaspekter

I de flesta IT-system är säkerheten central för att upprätthålla den funktion som systemet avses ha för verksamheten. Den klassiska CIA-triaden[1] med sekretess, riktighet och tillgänglighet ses ofta som grunden för säkerhetskraven, men det är viktigt att

[1] CIA står för de engelska orden *confidentiality*, *integrity* och *availability*.

även ta hänsyn till andra aspekter. Nivån på kravställningen för respektive säkerhetsaspekt måste baseras på en kombination av regelverk och verksamhetskrav för att nå ett tillräckligt och balanserat skydd av systemet och den information som systemet hanterar.

Sekretesskrav för hantering av klassificerad information är relativt lätt att ställa då dessa baseras på den informationssäkerhetsklass som systemet avses hantera. Även om systemet inte behandlar sekretessklassificerad information så finns ofta någon form av data i systemet som måste skyddas mot obehörig åtkomst, till exempel lösenord och interna kryptonycklar, vilket innebär att någon grad av sekretesskrav alltid finns på systemet.

Kraven på riktighet och tillgänglighet är ofta betydligt svårare att specificera än kraven på sekretess då tydliga regelverk saknas och händelser som påverkar dessa områden kan ge mer svårbedömda effekter på verksamheten. Ofta är systemets tillgänglighet kritisk för verksamheten samtidigt som informationshanteringen i systemet måste uppfylla kraven på riktighet och sekretess. I vissa fall förbättras flera aspekter av samma skyddsmekanism medan de i andra fall kan stå mot varandra. Exempelvis ger ett åtkomstskydd som primärt avses skydda sekretessen även ett skydd för informationens riktighet då det gör att endast betrodda användare kan förändra informationen i systemet. Ett exempel på en ökad risk som följd av en skyddsåtgärd är backuper som används för att förbättra tillgängligheten, trots att dessa ökar informationens exponering och därmed ökar problematiken kring sekretesskydd.

Ett IT-system består av och hanterar ett antal *tillgångar* som är skyddsvärda. En grundläggande typ av tillgång är den skyddsvärda information som systemet hanterar, exempelvis i form av dokument, kartbilder och databaser. Utöver detta finns i regel ett antal andra skyddsvärda informationstillgångar såsom lösenord, kryptonycklar och loggar. Även delar av systemet i sig kan utgöra tillgångar, exempelvis den mjukvara och hårdvara som systemet byggs upp av. Systemet och dess komponenter måste skyddas, delvis av sig självt och delvis genom sin omgivning, för att upprätthålla ett tillräckligt skydd av informationen och systemet.

I IT-system finns det en stor mängd potentiella säkerhetsrisker som måste bedömas och hanteras av systemen och deras miljö. Följande lista sammanfattar vanliga säkerhetsaspekter med exempel på generella risker kopplade till respektive säkerhetsaspekt.

- *Sekretess* (eng. *confidentiality*) – Obehörig åtkomst till tillgångar ska hindras.
  - Förlust av sekretessklassificerad information.
  - Förlust av annan skyddsvärd information, till exempel lösenord.
- *Riktighet* (eng. *integrity*) – Tillgångars riktighet ska bibehållas.
  - Manipulation av systemets funktionalitet.
  - Manipulation av information i systemet.

  - Manipulation av loggar.
  - Felaktig information kommer in och används i systemet.

- *Tillgänglighet* (eng. *availability*) – Tillgångar ska finnas tillgängliga när de behövs.

  - Partiella eller totala driftavbrott i systemet, som exempelvis innebär att användare inte når information på grund av fördröjningar i kommunikationen.
  - Systemet överbelastas så att information inte kan förmedlas genom systemet och därmed inte nå den som behöver informationen.

- *Innehav* (eng. *possession* el. *control*) – Tillgångar ska vara under kontroll av en betrodd part.

  - Ett krypterat lagringsmedia tappas bort eller stjäls. Effekten är att den som innehar minnet kan utföra attacker för att exempelvis dekryptera eller manipulera innehållet.
  - En server-hårdvara hanteras av obetrodda personer som kan manipulera utrustningen. Att obetrodda personer hanterat utrustningen innebär att det inte längre går att ha tilltro till utrustningens riktighet, det vill säga att tilltron har skadats oavsett om utrustningen har manipulerats eller inte.

- *Äkthet* (eng. *authenticity*) – Tillgångars ursprung ska vara säkerställda för att ha tilltro till dess utrsprungliga riktighet.

  - Information som saknar ursprungsmärkning, till exempel i form av digitala signaturer, kan komma från en obetrodd part och vara vilseledande.
  - Hårdvara, mjukvara och andra systemkomponenter med ospårbar leverantörskedja kan vara manipulerade och innehålla skadliga funktioner.

- *Användbarhet* (eng. *utility*[2]) – Tillgångar ska vara användbara och behålla avsedda värden för verksamheten.

  - Krypterad data för vilken nyckeln har förlorats kan inte dekrypteras och därmed inte användas i verksamheten.
  - Lagring av data på gamla typer av lagringsmedia kan innebära att data inte går att läsas och därmed inte kan användas.

- *Oavvislighet* (eng. *non-repudiation*) – Åtgärder ska knytas entydigt till en användare, på ett sätt så att denne inte kan förneka åtgärden.

[2] Ofta används den engelska termen *usability* i stället för utility. Utility är en tydligare term för nyttan hos en tillgång då usability även används för användbarhet i perspektivet hur lättanvända och lättförståeliga funktioner och system är för användaren.

- En användare kan inte knytas till sina aktiviteter på grund av bristfällig loggning eller logghantering.

Ovanstående lista är ett förslag på säkerhetsaspekter att ta hänsyn till i säkerhetsarbetet. CIA-triaden har kritiserats för att vara för enkel då flera aspekter vägs in under samma rubrik, till exempel ingår såväl äkthet som oavvislighet i riktighet. Faran är då att användningen gör att viktiga aspekter missas, vilket kan leda till att associerade risker inte identifieras och omhändertas.

Om CIA-triaden utökas med innehav, äkthet och användbarhet fås den så kallade *Parkerianska hexaden* (eng. *Parkerian hexad*) (Parker 2014), som har föreslagits som en mer relevant utgångspunkt för säkerhetsanalyser. Till skillnad från listan ovan så väger den Parkerianska hexaden in oavvislighet i aspekten äkthet.

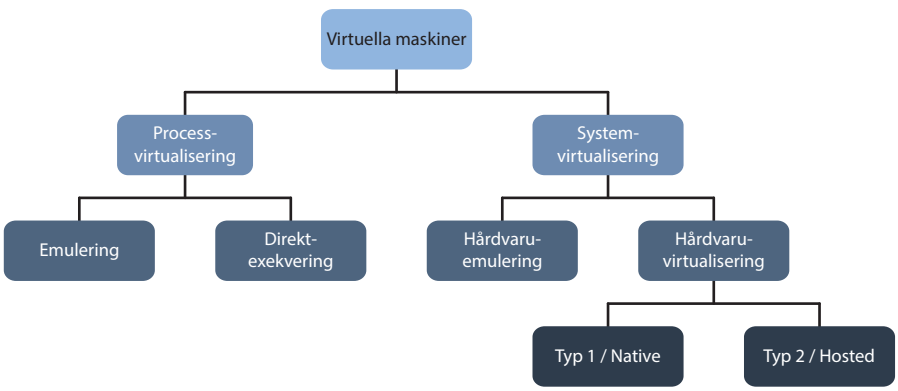
2 Bakgrund

Virtualisering av IT-system har sina rötter i 1960-talet, då tekniken användes för att separera användare i stordatorer. Sedan dess har antalet användningsområden växt och inkluderar nu ett flertal tekniker för olika nivåer och olika systemtyper. Virtualisering har nått omfattande spridning på senare år då virtualiseringsteknik har kommit i vardaglig användning, exempelvis för intrångsskydd i webbläsare, exekvering av Java-program och servervirtualisering i datacenter. Detta kapitel ger en översikt över virtualiseringstekniker och några av de fördelar som virtualisering kan ge.

2.1 Typer av virtualisering

Virtualisering är ett samlingsnamn för olika tekniker som skapar virtuella miljöer för mjukvara. Dessa tekniker bygger på några gemensamma principer, vilket illustreras av den taxonomi över olika virtualiseringstyper i IT-system som visas i figur 1. Denna taxonomi utgör en förenklad delmängd av den taxonomi som tagits fram av Pék, Buttyan och Bencsath (2013) i deras arbete med att sammanställa säkerhetsproblem i virtualiserade system.

Huvudgrupperna i taxonomin är *process-* respektive *systemvirtualisering*, baserat på omfånget av det som körs i den virtuella miljön. Enskilda processer körs i processvirtualiserade miljöer medan mjukvara för hela datorer körs i systemvirtualiserade miljöer.



Figur 1: Taxonomi för virtualiseringstekniker.

Programmeringsgränssnittet[3] bestämmer nästa nivå i taxonomin, där virtualiseringslagret och den underliggande hårdvaran kan exponera identiska eller olika programmeringsgränssnitt. Om programmeringsgränssnitten inte är lika måste virtualiseringsmiljön utföra en *emulering* av gästmjukvarans instruktioner så att motsvarande funktioner kan utföras med de instruktioner som finns tillgängliga i hårdvaran. När samma programmeringsgränssnitt exponeras kan gästmjukvaran köras direkt på den underliggande hårdvaran, så kallad *direktexekvering* (eng. *direct execution*).

Ett exempel på emulerad processvirtualisering är Java Virtual Machine (JVM), som används för att exekvera program skrivna i programspråket Java. Direktexevering kan exempelvis vara *sandboxing* av applikationer som används för att minska värdoperativsystemets exponering mot potentiellt skadliga applikationer. Sandboxing är vanligt förekommande i webbläsare, exempelvis i Google Chrome[4] och Mozilla Firefox[5], där tekniken bland annat används för att minska risken för spridning av skadlig kod från webbläsare till operativsystem. Exempel på en fristående sandbox för att köra godtyckliga program är Sandboxie[6].

Även systemvirtualisering kan utföras så att virtualiseringslagret emulerar ett annat programmeringsgränssnitt för att köra operativsystem och applikationer som är skrivna för en annan datorarkitektur än den faktiska hårdvaran. Ett exempel på emulerad systemvirtualisering är Bochs[7] som gör det möjligt att köra mjukvara skriven för x86-arkitekturer på andra underliggande arkitekturer, till exempel MIPS och ARM.

Systemvirtualisering som exponerar samma programmeringsgränssnitt, så kallad *hårdvaruvirtualisering*, kan antingen köras direkt på hårdvaran eller under värdoperativsystem. Dessa metoder saknar lämpliga svenska termer men kallas *typ 1* eller *native* (ungefär ”ursprunglig”) respektive *typ 2* eller *hosted* (ungefär ”värdbaserad”). Exempel på typ 1 är Xen[8], VMware ESX/ESXi[9] och Green Hills Integrity Multivisor[10]. Exempel på typ 2 är Oracle VirtualBox[11], KVM[12], VMware Workstation[13] och Microsoft Windows Virtual PC[14]. Typ 1 är den hårdvaruvirtualisering som normalt sett används på servrar medan typ 2 oftast används på arbetsstationer och kontorsdatorer.

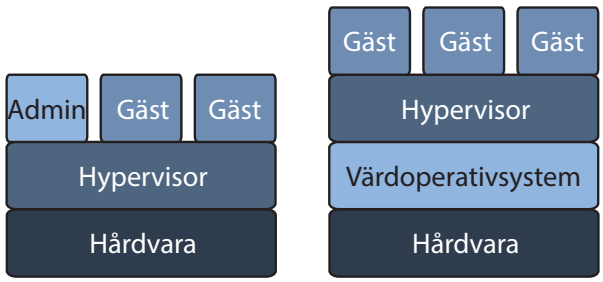
Virtualiseringslagret i systemvirtualisering kallas för *hypervisor* eller *virtual machine monitor* (VMM). Hypervisorn hanterar hårdvaran, implementerar virtuella system-

---

3 Programmeringsgränssnittet avser den instruktionsuppsättning och den programmeringsmodell som gäller för en processor.
4 https://www.google.com/chrome/
5 https://www.mozilla.org/sv-SE/firefox/
6 http://www.sandboxie.com/
7 Uttalas som ”box”, http://bochs.sourceforge.net/
8 http://www.xenproject.org/
9 http://www.vmware.com/
10 http://www.ghs.com/
11 https://www.virtualbox.org/
12 https://www.linux-kvm.org/
13 http://www.vmware.com/
14 http://www.microsoft.com/

funktioner som till exempel nätverksswitchar samt ger gästoperativsystemen tillgång till lämplig virtuell hårdvara såsom virtuella nätverkskort och grafikkort.

Figur 2 visar skillnaden på systemvirtualisering av typ 1 och typ 2. I typ 1 ligger hypervisorn direkt på hårdvaran och utgör således det enda mjukvarulager som normalt sett har direkt åtkomst till hårdvaran. I typ 2 finns ett värdoperativsystem som hanterar hårdvaran och hypervisorn körs i princip som en applikation under värdoperativsystemet. Upplägget i typ 2 innebär att värdoperativsystemet har kontroll över hypervisorn och därmed hela den virtualiserade miljön.



Figur 2: Typer av hypervisorer.

Vissa implementationer av systemvirtualisering typ 1 har en eller flera gäster med speciella privilegier, i figur 2 benämnd *Admin*, som har rättigheter att hantera hypervisorn och gästmiljöerna eller för att implementera specifika funktioner i den virtualiserade miljön. Ett exempel på en sådan admin-gäst är *värd-domänen* Dom0 under Xen, som avlastar funktioner från hypervisorn genom att hantera vissa drivrutiner för den fysiska hårdvaran och erbjuda tjänster som virtuella diskar och virtuellt nätverk till de övriga gästerna.

All virtualisering, såväl emulering som hårdvaruvirtualisering, innebär att det finns en viss mängd mjukvara mellan hårdvaran och den mjukvara som ska kapslas in i den virtuella miljön. Virtualiseringsmjukvaran konfigurerar hårdvaran så att åtkomsten begränsas mellan gästerna, samtidigt som den även tillhandahåller ett antal tjänster till gästerna, exempelvis nätverksåtkomst och ett lokalt användargränssnitt.

2.2 Fördelar med virtualisering

Systemvirtualisering kan ge fördelar i såväl server- som användarmiljön. Jämfört med system byggda direkt på fysiska servrar kan virtualiserade servermiljöer ge driftfördelar, framför allt genom bättre utnyttjande av hårdvaruresurser och förenklad drift av system. Genom den frikoppling som virtualisering ger mellan gästmiljöer och fysiska maskiner blir hanteringen av gäster (virtuella servrar) enklare. Exempelvis kan gäster enkelt skapas och tas bort, de kan *migreras* mellan olika fysiska servrar och fle-

ra gäster kan *samlokaliseras*[15] i samma fysiska server. Gäster kan även sparas i form av *ögonblicksbilder* (eng. *snapshots*) och *kloner*. Ögonblicksbilder och kloner kan användas för att skapa *återställningspunkter* och för att skapa nya gäster med samma egenskaper. Det senare används inom kommersiella molntjänster där det finns bibliotek med färdiga så kallade *virtual appliances*[16] som kan användas för att lösa användares behov med minimal konfiguration. En virtual appliance utgör en färdiginstallerad och förkonfigurerad lösning för ett specifikt ändamål, exempelvis en webbserver eller en databasserver.

Effekter som kan uppnås genom samlokalisering är exempelvis lägre energiförbrukning och högre utnyttjandegrad, något som leder till mindre mängd hårdvara samt mindre behov av fysiskt utrymme och kylning. Migreringsfunktionerna gör det enklare att underhålla den fysiska serverparken då gäster enkelt kan flyttas från den maskin som behöver underhåll. Migrering gör även uppgraderingar enklare då gästerna kan migreras när de nya fysiska servrarna är driftsatta varpå de gamla servrarna kan tas ur drift utan att störa funktionen. Genom frikopplingen mellan gäster och hårdvara finns även större möjligheter att fritt välja hårdvara vid uppgradering av serverparken.

I användarmiljön kan virtualisering också ge stora fördelar, till exempel genom möjligheten att köra klienter för flera system på samma fysiska hårdvara och genom att ge användare tillgång till samma arbetsyta[17], samma program och samma filer oavsett vilken dator eller bärbar enhet som nyttjas.

I detta avsnitt presenteras fem scenarion som visar på fördelar med virtualisering. Scenariona är generellt skrivna för att illustrera några av de möjligheter som ges med virtualisering av IT-system. Scenariona tar enbart upp fördelar med virtualisering då riskerna diskuteras i kommande kapitel. Dessutom tar scenariona inte hänsyn till Försvarsmaktens gällande regelverk för IT-säkerhet, vilket kan medföra att de inte är realiserbara med dagens teknik.

2.2.1 Platsbesparing

En av de potentiella fördelarna med virtualisering är platsbesparing, speciellt för servermiljöer där många servrar som tidigare var fysiska kan ersättas med virtuella servrar som samlokaliseras på ett mindre antal fysiska maskiner. När nya virtuella servrar kan läggas till utan att öka antalet fysiska maskiner går det att ha dedikerade virtuella servrar med anpassad konfiguration för respektive funktion, något som underlättar administration av de olika funktionerna då beroenden mellan dem undviks. Det maximala antalet virtuella maskiner begränsas i huvudsak av tillgänglig prestanda i

---

15 Det är vanligt att de engelska termerna för samlokalisering, *co-location* och *co-residence*, används även på svenska.

16 Det saknas en bra svensk term för detta. *Virtual appliance* betyder ungefär ”virtuell apparat” eller ”virtuell tillämpning”.

17 Även kallat *skrivbord*, *workspace* eller *desktop*, det vill säga den miljö som användaren ser och upplever när denne använder datorn.

värdmaskinerna, exempelvis i form av lagringsutrymme, processorkraft och arbetsminne.

Virtualiseringstekniken ger möjlighet till platsbesparing även på operatörernas arbetsplatser[18], genom att en fysisk terminal inklusive tangentbord, mus, skärm med mera kan anslutas mot flera olika serversystem. Genom att använda en infrastruktur för *virtuella arbetsytor*[19] flyttas behovet av exempelvis beräkningskraft till serversidan och användare kan använda en *tunn klient*[20] eller en *nollklient*[21] på arbetsplatsen. Samma klient kan potentiellt användas för att ansluta till flera serversystem vilket eliminerar behovet av flera datorer med separata skärmar och inmatningsenheter på arbetsplatsen. Minskat behov av hårdvara på arbetsplatsen sparar utrymme och minskar elförbrukningen, något som kan förbättra såväl arbetsplatsens ergonomi som miljö.

I militära sammanhang är förenklad omgruppering en ytterligare fördel som kommer med minskad mängd hårdvara, då det innebär att mindre mängd utrustning behöver hanteras.

> *Scenario:* En operatör i något av Försvarsmaktens system sitter vid en terminal med ett tangentbord och en mus samt en eller flera skärmar som är sammankopplade till en stor arbetsyta. Terminalen ger operatören tillgång till flera samtidiga system, vilket gör att denne inte längre behöver ha separata tangentbord, möss och skärmar för de olika systemen. När operatören behöver tillgång till ett specifikt system antingen startar eller loggar denne in på en virtuell server som bara kör det systemet. Operatören kan enkelt arrangera de olika virtuella skrivborden på terminalens arbetsyta. Varje fönster kan anpassas storleksmässigt utifrån aktuellt behov av överblick och läsbarhet. System med olika sekretessgrad kan användas sida vid sida och varje enskild operatör kan själv anpassa arbetsytan utifrån egna preferenser. Operatörer kan också dela uppgifter mellan sig vid behov genom att en operatör överlåter en virtuell maskin till en annan operatör, något som går snabbt då virtualiseringen är serverbaserad och det bara krävs ut- och inloggning. På så sätt kan operatörernas kapacitet utnyttjas bättre, de behöver inte flytta sig fysiskt och det ger därmed kortare avbrott vid förändringar.

---

18 Operatörernas arbetsplatser kan vara lokaliserade i många olika miljöer, exempelvis i kontorsmiljö, i ett fordon, ombord på ett fartyg eller i ett stabstält.

19 Eng. *virtual desktop infrastructure (VDI)*.

20 En tunn klient (eng. *thin client*) utgör en enkel dator som används som terminal mot en server, vanligtvis utan lokal lagring av användardata. Tunna klienter har en viss processorkraft och innehåller i regel någon form av operativsystem.

21 En nollklient (eng. *zero client*) är en minimal klient som inte innehåller någon egen beräkningskraft eller lagring, utan bara utgör en enhet för presentation av skärmbild och inmatning. All beräkning och databehandling inklusive rendering av skärmbilden sker på serversidan.

2.2.2 Snabb anpassningsförmåga

Då virtuella maskiner kan skapas och tas bort relativt enkelt så kan ett virtualiserat system vara lättare att anpassa under drift. Avbildningar för relevanta funktioner kan finnas förberedda för installation vid behov. Genom separationen mellan de virtuella maskinerna behöver inte systemadministratörerna ta så stor hänsyn till beroenden som skulle uppstå mellan olika applikationer, operativsystem, delade mjukvarubibliotek och andra delade resurser om maskinerna inte separerades.

De virtuella maskinerna kan även ha olika konfigurationer av virtuell hårdvara, som i sin tur är knuten olika hårt till den fysiska hårdvaran. Genom detta kan till exempel mängden arbetsminne samt antalet nätverkskort, hårddiskar, processorkärnor och usb-portar varieras. Om behovet av antalet samtidigt körande virtuella maskiner ökar och överskrider hårdvarukraven kan standardiserad hårdvara införskaffas för att öka kapaciteten i systemet.

Standardiserad hårdvara kan användas även på operatörernas arbetsplatser, vilket underlättar om antalet arbetsplatser behöver utökas. I vissa virtualiseringssystem går det att ansluta via webbaserade gränssnitt, vilket ger en teoretisk möjlighet att skapa en ny operatörsplats med hjälp av vilken hårdvara som helst så länge den har kapacitet nog att köra en webbläsare.

> *Scenario:* Vid internationell samverkan underlättar virtualisering byten mellan olika koalitioner. Ett typiskt exempel är ett av marinens fartyg som deltar i en samnordisk övning, för att sedan delta i internationella uppdrag inom FN och NATO. Vid varje tillfälle krävs en specifik roll med unika krav på samverkan mellan de deltagande styrkorna, vilket även ställer krav på vilka IT-system som finns i drift ombord.
>
> Genom att systemen är virtualiserade kan de bytas ut mot system med de förmågor som krävs för stunden. De virtualiserade systemen kan installeras, konfigureras och testas i förväg på annan plats och sedan föras över till fartyget i form av kloner vid behov. Det är även enkelt att anpassa och förändra uppsättningen av system under pågående uppdrag genom att ladda ner och starta nya virtuella maskiner. På samma sätt kan även system i form av virtuella maskiner lånas eller flyttas mellan parterna i koalitionen.

2.2.3 Förenklad återställning

Genom möjligheten att ta ögonblicksbilder av de virtuella maskinerna blir återställningsarbetet enklare efter oönskade händelser, såsom cyberangrepp och olyckshändelser. Virtualiseringen innebär att återställningen underlättas även om hårdvaran förstörts, genom att virtualiseringslagret tar bort mycket av beroendet mellan den virtuella och den fysiska hårdvaran. De virtuella maskinerna kan således återställas på annan fysisk hårdvara.

Om systemet behöver återställas på grund av cyberangrepp så kan den svaghet som utnyttjades åtgärdas temporärt innan systemet åter tas i skarp drift. Under tiden som det temporära systemet används kan en kopia av maskinen uppdateras i en skyddad miljö. Den uppdaterade maskinen kan sedan ersätta den temporära så fort uppdateringen är klar. Genom täta säkerhetskopior och ögonblicksbilder kan mindre mängd användardata förloras även om den virtuella maskinen blir obrukbar i samband med angrepp.

Om det är praktiskt möjligt, exempelvis avseede sekretessklassificerad information i systemet, finns även möjlighet att isolera en angripen maskin och låta den vara i fortsatt drift som en *honungsfälla*[22] för att avleda angriparen. På så sätt kan angriparen studeras i realtid i en avgränsad miljö, samtidigt som en virtuell ersättningsmaskin patchas och härdas för att återuppta skarp drift.

Kloning kan användas för att stärka säkerheten vid distribution av mjukvaran, genom att system kan installeras, konfigureras och valideras i kontrollerad miljöer för att sedan spridas i form av identiska kopior till de ställen de ska användas. Innan en mottagen kopia tas i bruk kan riktigheten kontrolleras genom att en hashsumma av kopian jämförs mot en hashsumma som beräknades innan maskinen skickades.

> *Scenario:* Ett pågående intrångsförsök upptäcks i ett ledningssystem vid ett kritiskt skede av en insats. Angriparen kringgår systemets skyddsmekanismer en efter en och det är frågan om minuter innan angriparen har nått administratörsrättigheter i systemet. Intrånget sker via en nätverkskoppling som inte kan kopplas ner på grund av den pågående insatsen. Ansvarig chef fattar beslut om att en alternativt konfigurerad virtuell enhet ska användas som temporär ersättning under tiden den nuvarande säkras. Det finns flera alternativa enheter att välja mellan, alla i form av virtuella maskiner, som kan installeras medan insatsen pågår utan avbrott och större störningar. Den virtuella enhet som angripits fryses i sitt nuvarande läge och skickas för forensisk analys till MUST, medan en ögonblicksbild av maskinen från innan angreppet patchas för att åter användas i systemet.

2.2.4 Dynamisk skalning

Systemvirtualisering av servrar innebär att virtuella servrar kan läggas till, tas bort, startas och stoppas automatiskt beroende på systemets belastning. Det är relativt enkelt att tillföra och ta bort hårdvara för att hantera belastningsändringar över tid. Virtualiseringslagret tar även bort mycket av beroendet mellan den virtuella och den faktiska hårdvaran, något som underlättar utbyggnad då ny hårdvara inte behöver vara identisk med den befintliga för att systemet ska fungera.

Om flera system delar på ett antal fysiska maskiner går det att göra en dynamisk skalning (omprioritering) mellan systemen för att ge bäst övergripande prestanda, det vill

[22] Eng. *honeypot*, datorer som sätts upp för att locka till sig angrepp eller avleda angripare från det verkliga målet.

säga att öka antalet virtuella servrar av den typ som för tillfället behövs och samtidigt minska ner antalet virtuella servrar med andra uppgifter.

De virtuella servrarnas hårdvarubestyckning kan snabbt förändras. Det som krävs är en ny konfiguration och en eventuell omstart av den virtuella maskinen. På så sätt går det relativt enkelt att till exempel öka antalet tillgängliga nätverkskort, ändra mängden minne och antalet processorer hos den virtuella maskinen. Den begränsande faktorn är att den sammanlagda utnyttjade prestandan hos de virtuella maskinerna aldrig kan överstiga den totala prestandan hos den fysiska hårdvaran.

> *Scenario:* Beroende på aktuella operationer och insatser varierar Försvarsmaktens behov av server- och systemresurser över tid. Genom att använda virtuella systemservrar kan resursmängden varieras dynamiskt i serverhallen. På så sätt kan resursutnyttjande effektiviseras utan att ny hårdvara behöver införskaffas varje gång. Det gör också att mängden hårdvara som krävs för att köra de system som används minskar i och med att hårdvaruresurserna utnyttjas effektivare. Om behov uppstår av mer hårdvara kan den installeras och snabbt tas i användning, utan att särskild anpassning behöver göras utifrån något specifikt systems hårdvarukrav. Virtualiseringen medger att COTS med fördel används vid hårdvaruuppgraderingar, vilket sparar tid och pengar.

2.2.5 Testning i virtualiserad miljö

Virtualiserade miljöer är särskilt lämpade för testning av system- och nätverkskonfigurationer i och med att ny virtuell hårdvara enkelt kan skapas, sparas och återanvändas. Möjligheten att spara ögonblicksbilder av virtuella system underlättar testning, på motsvarande sätt som versionshantering underlättar programutveckling. När en ny variant av ett system ska testas tas en ögonblicksbild av systemet och sedan utförs testet. Om testet inte lyckas är det enkelt att återställa systemet med stöd av ögonblicksbilden, göra nödvändiga förändringar, ta en ny ögonblicksbild och utföra ett nytt test.

Utöver användning av ögonblicksbilder vid testning går det enkelt att parallellisera tester genom att en virtuell grundmaskin klonas, varefter varje klon förändras i enlighet med testupplägget. Klonerna kan sedan testas parallellt, förändras ytterligare, klonas igen och så vidare.

I och med att virtualiserade miljöer är så väl lämpade för testning är en komplett uppräkning av alla användningsmöjligheter svår att åstadkomma. Några exempel på Försvarsmaktsrelevant testning som kan göras i virtuell miljö är tester av nya system, funktionsuppdateringar, säkerhetsuppdateringar, alternativa konfigurationer och skyddsåtgärder vid angrepp. Testsystemet kan även användas vid övningar och tester av scenarion för incidenthantering.

> *Scenario:* Innan en utlandsstyrka upprättar sin camp kan den blivande systemmiljön testas under realistiska förhållanden genom att testsystem byggs

upp. Testsystemen kan användas för att undersöka IT-säkerheten och systemens beteende i olika situationer, exempelvis vid trafkstörningar och när hårdvara fallerar. Genom att nyttja virtualisering kan det validerade systemet sedan enkelt klonas till de platser där det ska användas och säkerhetskopior kan lagras för senare behov. Eftersom spridningen kan ske över nätverk förkortas tiden mellan färdig validering och faktisk driftsättning.

Genom att behålla testsystemet även när campen har upprättats kan uppdateringar av programvaran testas och valideras i en säker och kontrollerad miljö. Den uppdaterade mjukvaran kan sedan överföras till campens system.

Vid en incident, exempelvis ett pågående intrångsförsök i ett av campens ledningssystem, kan testsystemet användas för att snabbt testa olika skyddslösningar. Genom att systemet är virtualiserat kan en uppdaterad version snabbt överföras till utlandsstyrkan för att säkra upp systemet mot intrångsförsöket. I testsystemet kan olika angreppsscenarion och motmedel testas för att ytterligare förbereda och förbättra skyddet av systemen.

3 Litteraturöversikt

En litteraturstudie har genomförts för att erhålla en översikt av forskningsläget vad gäller sårbarheter och säkerhetsproblematik i virtualiserade miljöer. Litteraturen har identifierats genom strukturerade sökningar i databaser över vetenskapliga publikationer. För att begränsa urvalet har enbart publikationer daterade 2008 och senare tagits med, vilket även ger en rimlig avgränsning med tanke på den snabba utvecklingen av virtualiseringstekniken under de senaste åren.

3.1 Scopus

En sökning på Scopus[23] med nyckelorden ”security”, något av orden ”virtualization” eller ”virtual” samt något av orden ”vulnerability” eller ”separation” [24] gav 581 träffar daterade år 2008 och senare.

Dessa 581 träffar filtrerades manuellt, där det första steget baserades på titeln. Efter detta återstod 120 träffar för vilka samtliga sammanfattningar lästes igenom, varpå en ytterligare gallring gjordes. Efter denna gallring återstod 31 träffar som lästes igenom utförligare för att välja ut de mest relevanta. Slutligen ansågs 15 stycken artiklar ha tillräckligt relevant innehåll för att användas som underlag i rapporten. De utvalda artiklarna är:

- M. Ali, S. U. Khan och A. V. Vasilakos (2015). ”Security in cloud computing: Opportunities and challenges”. I: *Information Sciences* 305, s. 357–383. DOI: 10.1016/j.ins.2015.01.025

- S. N. Brohi m. fl. (2012). ”Identifying and analyzing security threats to virtualized cloud computing infrastructures”. I: *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management, ICCCTAM 2012*, s. 151–155. DOI: 10.1109/ICCCTAM.2012.6488089

- R. C. Chiang m. fl. (2015). ”Swiper: Exploiting virtual machine vulnerability in third-party clouds with competition for I/O resources”. I: *IEEE Transactions on Parallel and Distributed Systems* 26.6, s. 1732–1742. DOI: 10.1109/TPDS.2014.2325564

[23] SCOPUS är en databas som sammanställer vetenskapliga publikationer från ett stort antal konferenser och tidskrifter. Databasen omfattar publikationer från bland annat IEEE, ACM, Springer, Elsevier och Wiley.

[24] TITLE-ABS-KEY (security AND (virtualization OR virtual) AND (vulnerability OR separation)) AND (LIMIT-TO(SUBJAREA,"COMP")) AND (LIMIT-TO(LANGUAGE,"English")), sökning genomförd 2017-05-31.

- A. Everspaugh m. fl. (2014). ”Not-So-Random numbers in virtualized Linux and the Whirlwind RNG”. I: *Proceedings - IEEE Symposium on Security and Privacy*, s. 559–574. DOI: 10.1109/SP.2014.42
- K. Hashizume m. fl. (2013). ”An analysis of security issues for cloud computing”. I: *Journal of Internet Services and Applications* 4.1, s. 1–13. DOI: 10.1186/1869-0238-4-5
- R. Hörmanseder och M. Jäger (2014). ”Cloud security problems caused by virtualization technology vulnerabilities and their prevention”. I: *IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks*, s. 373–383
- Y.-L. Huang m. fl. (2012). ”Security impacts of virtualization on a network testbed”. I: *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability, SERE 2012*, s. 71–77. DOI: 10.1109/SERE.2012.17
- G. Irazoqui m. fl. (2015). ”Fine grain Cross-VM attacks on Xen and VMware”. I: *Proceedings - 4th IEEE International Conference on Big Data and Cloud Computing, BDCloud 2014 with the 7th IEEE International Conference on Social Computing and Networking, SocialCom 2014 and the 4th International Conference on Sustainable Computing and Communications, SustainCom 2014*, s. 737–744. DOI: 10.1109/BDCloud.2014.102
- G. Irazoqui m. fl. (2014). ”Wait a minute! A fast, cross-VM attack on AES”. I: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8688 LNCS, s. 299–319. DOI: 10.1007/978-3-319-11379-1_15
- B. K. Mughal, A. Syed och A. Khan (2014). ”Information leakage in the cloud”. I: *ICOSST 2014 - 2014 International Conference on Open Source Systems and Technologies, Proceedings*, s. 56–61. DOI: 10.1109/ICOSST.2014.7029320
- G. Pék, L. Buttyan och B. Bencsath (2013). ”A survey of security issues in hardware virtualization”. I: *ACM Computing Surveys* 45.3. DOI: 10.1145/2480741.2480757
- D. Perez-Botero, J. Szefer och R. B. Lee (2013). ”Characterizing hypervisor vulnerabilities in cloud computing servers”. I: *Cloud Computing 2013 - Proceedings of the 2013 International Workshop on Security in Cloud Computing*, s. 3–10. DOI: 10.1145/2484402.2484406
- T. Ristenpart m. fl. (2009). ”Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds”. I: *Proceedings of the ACM Conference on Computer and Communications Security*, s. 199–212. DOI: 10.1145/1653662.1653687

- F. Rocha, T. Gross och A. Van Moorsel (2013). ”Defense-in-depth against malicious insiders in the cloud”. I: *Proceedings of the IEEE International Conference on Cloud Engineering, IC2E 2013*, s. 88–97. DOI: 10.1109/IC2E.2013.20

- F. Zhou m. fl. (2013). ”Scheduler vulnerabilities and coordinated attacks in cloud computing”. I: *Journal of Computer Security* 21.4, s. 533–539. DOI: 10.3233/JCS-130474

I vissa fall har ytterligare källor använts, men då för att ta del av ytterligare detaljer kring risker och sårbarheter. Dessa har primärt lokaliserats genom referenser i ovanstående källor. Samtliga referenser som används i texten återfinns i litteraturlistan i slutet av rapporten.

En notering vid genomläsningen av litteraturen är att många källor handlar om säkerhet för molntjänster (eng. *cloud computing*), vilket är ett betydligt bredare område än virtualisering. Systemvirtualisering ingår som en komponent i de arkitekturer som normalt används för molntjänster vilket gör att säkerhetsforskningen kring virtualisering i många fall drivs av säkerhetsaspekter för molnsystem.

3.2 FOI-rapporter

Sökningar[25] har gjorts i FOI:s öppna rapportdatabas, först med nyckelordet ”virtual*” (täcker exempelvis ”virtualisering”, ”virtual”, ”virtualisation”, ”virtualization”) som ger 14 träffar. Med nyckelordet ”virtuell*” fås sju träffar varav fem av dessa även ingår i resultatet från den första sökningen.

Av de totalt 16 unika träffarna handlar åtta rapporter om andra områden än IT-virtualisering, till exempel virtuella prototyper av ubåtar. Efter en genomgång av innehållet i de kvarvarande åtta rapporterna återstår två som har relevant innehåll för denna litteraturöversikt. Dessa rapporter är:

- A. Bengtsson och L. Westerdahl (2009). *Virtual Machines - Security Qualities*. Tekn. rapport FOI-R--2904--SE. FOI, Totalförsvarets Forskningsinstitut

- H. Karlzén (2012). *Molnet - möjligheter och begränsningar*. Tekn. rapport FOI-R--3381--SE. FOI, Totalförsvarets Forskningsinstitut

Båda rapporterna har annat huvudfokus än säkerhetsproblem i virtualiserade miljöer vilket gör att detta specifika område ges relativt lite utrymme i rapporterna. Bengtsson och Westerdahl (2009) begränsar diskussionen om risker i virtualiserade system

[25] Sökning genomförd 2017-05-31.

till att referera ett arbete av Ormandy (2007), där säkerheten i sex olika virtualiseringssystem undersöktes. Ormandys undersökning ledde fram till slutsatsen att alla testade virtualiseringssystem hade sårbarheter som kunde nyttjas på ett eller annat sätt. Referensen är äldre än den satta tidsramen för denna litteraturöversikten och inkluderas därmed inte.

Karlzén (2012) skriver övergripande om vad molnet och molntjänster är samt om riskområden som finns i molnbaserade system. Några få risker som förekommer i virtualiserade miljöer beskrivs kortfattat, däribland kloning av maskiner och samlokalisering med angripares maskiner. Dessa risker tas upp i större detalj i andra referenser i litteraturöversikten.

4 Risker med virtualiseringsteknik

Virtualiserade miljöer innebär flera driftfördelar, men även en ökad exponering för risker kopplade till såväl sårbarheter som felaktigt handhavande. Ett antal risker tillkommer när virtualiseringstekniken används för att implementera IT-system och dessa risker måste hanteras på ett medvetet och strukturerat sätt för att uppnå en acceptabel säkerhetsnivå hos driftsatta system.

Sårbarheter som finns i icke-virtualiserade miljöer kvarstår när system virtualiseras, vilket innebär att virtualiseringen inte bidrar direkt till ökad säkerhet för gästmiljöerna jämfört med installation på fysiska servrar. Att införa virtualisering sänker snarare säkerhetsnivån i det generella fallet (Symantec 2012).

4.1 Tekniska risker

Vid virtualisering tillkommer de funktioner som utgör virtualiseringsmiljön, till exempel hypervisorn och virtuella nätverkskomponenter. Hypervisorn är en felkritisk systemdel[26] när det gäller att upprätthålla separationen mellan gästoperativsystem (Symantec 2012). Den virtualiserade miljön har även större komplexitet än en fysisk motsvarighet då mjukvaran i virtualiseringslagret tillkommit med medföljande sårbarheter.

Virtualiserade miljöer använder ofta virtuella nätverkskomponenter som körs under hypervisorn. Dessa nätverkskomponenter kan innehålla sårbarheter som påverkar det virtuella nätverket, till exempel genom läckage mellan VLAN, men det kan även finnas sårbarheter som kan påverka hypervisorn via det virtuella nätverket.

Utöver virtuella nätverkskomponenter finns andra virtualiserade komponenter i systemet, exempelvis grafikkort, ljudenheter och USB-funktioner. Samtliga virtuella komponenter kan innehålla sårbarheter som kan påverka hypervisorn eller separation av gäster.

En av fördelarna med virtualisering är att flera virtuella maskiner kan dela på den prestanda som finns i den fysiska maskinen för att få bättre utnyttjande av hårdvaran. Detta kan dock leda till problem med vissa skyddsåtgärder som används i fysiska miljöer, då dessa till stor del bygger på att maskinerna har överprestanda som används till att exekvera skyddsåtgärder. Ett exempel på en skyddsåtgärd är antivirusmjukvara som regelbundet genomsöker arbetsminne och filer samt kontinuerligt kontrollerar data som läses från och skrivs till olika media. Antivirusmjukvaran använder således en viss mängd resurser på respektive virtuell maskin i form av lagring, arbetsminne och processorkraft som då inte kan nyttjas av de funktioner vars syfte motiverar systemets existens. Dessutom kör antivirusmjukvaran i regel schemalagda systemgenomsökningar och nedladdningar av uppdaterad virusdatabas. Om antivirusmjukvara schemaläggs samtidigt

[26] Felkritisk systemdel: eng. *single point of failure*.

på flera samlokaliserade virtuella maskiner kan detta leda till att hårdvaran överbelastas, vilket kan medföra att systemet blir otillgängligt (Kaspersky u.å.).

Beroende på hur systemen utformas så kan allokering av virtuella maskiner till hårdvara vara kritisk för hur säkerheten upprätthålls i systemen. Om virtuella maskiner med olika säkerhetskrav[27] delar fysiska resurser så ökar risken för intrång och skada på maskiner med högre kravnivå från virtuella maskiner med lägre kravnivå. Exempel på delade resurser är såväl fysisk hårdvara som lagringsnätverk (SAN[28]).

4.2 Administrativa risker

I miljöer med virtualiserade servrar som hanterar skilda verksamhetssystem är det viktigt att tydligt fördela ansvar mellan olika aktörer i miljön. Det är centralt att tydliggöra vilket ansvar respektive part har i såväl drifts- som säkerhetsfrågor för att systemet ska hålla en kontinuerligt hög säkerhetsnivå.

Systemadministratörer utgör en kritisk grupp i miljöer baserade på virtualiserade servrar, likaväl som i miljöer baserade på fysiska servrar. I virtualiserade miljöer finns ytterligare administrativa funktioner utöver de som finns i icke-virtualiserade miljöer, bland annat administration av virtualiseringsmiljöns funktioner.

I virtualiserade miljöer är det enkelt att definiera administratörsroller med för omfattande åtkomst till systemet då hela infrastrukturen hänger ihop (PCI 2011). I högkritiskta system bör *separation of duty*[29] appliceras så att kritiska operationer inte kan utföras av enskilda systemadministratörer och användare. På samma sätt bör *least privilege*[30] appliceras genomgående i kritiska system för att undvika att systemadministratörer och användare får behörighet att utföra åtgärder i systemet som dessa inte borde få genomföra. I vissa situationer kan separation of duty och least privilege hamna i konflikt med krav på till exempel tillgänglighet, vilket medför att andra åtgärder måste vidtas. Ett exempel på ett sådant situation är sjukvården där det är viktigare att personalen kommer åt patientjournalerna än att patienternas personliga integritet värnas fullt ut. I detta fall används uppföljning och spårbarhet för att säkerställa att personalen inte läser journaler som de inte är behöriga till, snarare än att tillgången begränsas med tekniska medel.

---

27 En term som används för att särskilja olika nivåer på säkerhetskraven är ”förtroendenivå” (eng. *trust level*). Denna term används exempelvis av Payment Card Industry (PCI) Security Standards Council, ett samarbetsorgan för säkerhet i betalningssystem (PCI 2011).

28 SAN, eng. *storage area network*.

29 *Separation of duty*, sv. ungefär fördelning av uppgifter eller fördelning av ansvar, innebär att arbetsuppgifterna ska fördelas så att ingen ensam person kan åsidosätta säkerheten i systemet eller kringgå de rutiner som systemet ska upprätthålla. Ett vanligt exempel är att en person kan registrera en inkommen faktura i ett ekonomisystem men att en annan person måste attestera den för att betalning ska ske. Detta förfarande hindrar en ensam person från att exempelvis registrera falska fakturor för att själv ta pengarna.

30 *Least privilege*, sv. ung. minsta behörighet, innebär att en person inte ska ha befogenheter som denne inte behöver ha i systemet. Exempelvis behöver normalt sett inte vanliga användare ha administratörsbehörighet på de datorer de använder.

För virtualiserade miljöer kan problem med breda roller bli omfattande då administrationen på virtualiseringsnivån omfattar många virtuella maskiner och att åtkomst därmed ges till många virtualiserade system om dessa delar miljö. Ofta finns flera administrativa funktioner för att hantera till exempel virtualiseringsmiljön, migrering av virtuella maskiner och den fysiska hårdvaran vilket innebär att personal som hanterar dessa funktioner kan ha åtkomst till samtliga virtuella maskiner i miljön.

Den mer komplexa miljö som virtualiseringen innebär leder till nya risker i samband med att administrativa åtgärder genomförs. Misstag i administrationen av virtualiseringsmiljön kan leda till att samtliga system i miljön slås ut samtidigt och i värsta fall kan fel även propagera till andra datacenter som i fallet[31] med Amazons molntjänst EC2[32]. En felaktigt konfigurerad router ledde till att ett stort antal virtuella maskiner samtidigt försökte migrera till annan hårdvara vilket gjorde delar av molntjänsten otillgänglig under ett antal timmar. Dessutom gick ett mindre antal av de virtuella maskinerna inte att återställa korrekt vilket ledde till dataförlust för ett antal kunder.

Genom virtualiseringens funktioner för att ta ögonblicksbilder av virtuella maskiner och att migrera virtuella maskiner mellan fysiska värdar kan hantering och lagring av de virtuella maskinerna ske på ett flertal platser i systemet. För att undvika att skyddsvärd information hanteras och lagras felaktigt måste de administrativa rutinerna säkerställa att exempelvis diskavbildningar och migration görs och hanteras på ett lämpligt sätt för att undvika oönskad exponering utanför de skydd som tillhandahålls i den tekniska miljön.

31 https://aws.amazon.com/message/65648/

32 Amazon EC2 (Elastic Compute Cloud) är en tjänst där kunder hyr kapacitet i form av virtuella servrar.

5 Angreppsvägar

Detta kapitel tar upp olika potentiella angreppsvägar som förekommer i virtualiserade miljöer samt exempel på rapporterade sårbarheter för dessa angreppsvägar. Följande beskrivning utgår från den struktur som Pék, Buttyan och Bencsath (2013) använder, men kategoriserar angreppen även utifrån om de är interna angrepp, nätverksangrepp eller övriga angrepp, baserat på angiparens åtkomst till systemet vid tillfället för det specifika angreppet. Ett internt angrepp görs av angripare som redan är inne i systemet, till exempel i en gäst eller en värd. Nätverksangrepp avser angrepp där angripare befinner sig utanför systemet och inte nödvändigtvis har några privilegier i detta, men kan nå systemet via ett nätverk. Övriga angrepp avser angrepp via andra gränsytor, till exempel via fysisk åtkomst eller genom administrativa funktioner för virtualiseringsmjukvaran.

Sårbarheterna som tas upp i detta kapitel är i regel sådana att angripare inte kan göra externa angrepp och direkt få kontroll över centrala funktioner i system, såsom exempelvis hypervisorn. Sårbarheterna går däremot att länka samman genom att flera sårbarheter nyttjas för att åstadkomma ett mer komplext och potent angrepp. Detta illustreras av Perez-Botero, Szefer och Lee (2013) som visar hur ett antal kända sårbarheter i KVM och Xen tillsammans kan bygga upp olika angreppsvägar för att nå till önskat djup i systemet.

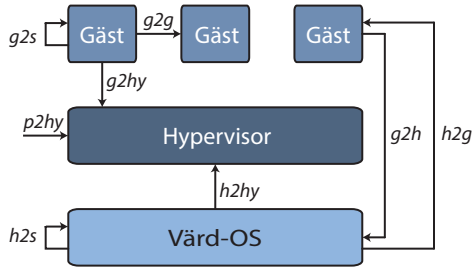
För tydlighets skull ses samtliga sårbarheter som enskilda, även om de i praktiken kan användas i en kedja av angrepp för att nå ett specifikt mål. Fördelen med detta synsätt är att alla sårbarheter kan kategoriseras separat, dock med effekten att angripare som nyttjar en kedja av sårbarheter då kommer att ändra roll baserat på den åtkomst till systemet som dessa har vid respektive punkt i angreppskedjan. Exempelvis byter en extern angripare som tar sig in i systemet roll till att vara en intern angripare för nästa steg i kedjan.

5.1 Interna angrepp

Figur 3 visar de olika angreppsvägarna för interna angrepp mot den virtualiserade miljön och dess värd respektive gäster. Namnen på angreppsvägarna är hämtade från Pék, Buttyan och Bencsath (2013) och indikerar vilken angreppsväg som avses. Figur 3 visar virtualisering av typ 2 (se avsnitt 2.1) men den principiella skillnaden för typ 1 är att värd-OS där kan liknas med en gäst med kraftigt utökade privilegier i systemet.

5.1.1 g2g: Guest-to-guest

Det är ovanligt med angrepp via virtualiseringssystemet som ger en gäst direkt tillträde till en annan gäst. Däremot finns det ett antal olika angrepp som kan ge tillgång till information om offret eller påverka denne. En typ av angrepp är så kallad memo-



Figur 3: Interna angreppsvägar för systemvirtualisering typ 2.

ry deduplication attacks[33] där en gäst kan få reda på viss information om att specifika applikationer körs på den andra gästen (Ristenpart m. fl. 2009). Denna information kan sedan användas för att ytterligare angripa en gäst, till exempel genom en överbelastningsattack[34] eller genom att göra ett angrepp mot schemaläggaren i virtualiseringslagret. Schemaläggaren är den funktion i systemet som fördelar systemets processortid till de processer som körs.

Angrepp mot schemaläggaren beskrivs av Zhou m. fl. (2013) och Chiang m. fl. (2015) som ett sätt att, med minimalt utnyttjande av systemresurser, genomföra en partiell degradering av en annan gästs prestanda. Detta är speciellt intressant i vissa kommersiella molntjänster, till exempel Amazon EC2, som tar betalt baserat på resursutnyttjande och där angripare enkelt kan skaffa sig egna virtuella maskiner.

Sidokanaler kan nyttjas vid angrepp för att få tag i information från en annan gäst, till exempel kryptonycklar. Irazoqui m. fl. (2014) och Irazoqui m. fl. (2015) visar att det går att delvis få fram AES-nycklar ur välkända kryptobibliotek som körs i en annan gäst genom angrepp där processorcachens egenskaper utnyttjas för att få ut information om exekveringen av kryptoalgoritmen. I virtualiserade miljöer blir ”brusnivån” i den information som fås via processorcachen högre vilket gör angreppet mindre effektivt än om det genomförts i samma gäst eller på samma icke-virtualiserade dator. Trots den lägre effektiviteten får angreppet ändå fram tillräckligt med information för att åsidosätta säkerheten i kryptot. Vissa typer av dessa angrepp är relativt lätta att motverka genom att implementera specifika skyddsmekanismer i kryptoalgoritmen, vilket också görs i ökande utsträckning i kryptobiblioteken. Irazoqui m. fl. (2015) visar resultat där de får ut c:a 40–60 av 128 bitar i nyckeln i en kontrollerad virtuell miljö medan de får ut c:a 35 bitar av nyckeln vid experiment i Amazons EC2-molntjänst.

[33] *Memory deduplication*, sv. ungefär undvikande av minnesduplicering, innebär att flera virtuella maskiner delar minnesområden med identiskt innehåll. Detta kan typiskt vara i en operativsystemskärna eller annan mjukvara som körs på flera maskiner. Vid en skrivning till minnesområdet skapas en kopia som används enbart av den skrivande maskinen.

[34] Eng. *denial of service attack* (DoS-attack).

Sidokanaler kan även användas för att kommunicera mellan virtuella maskiner, till exempel från malware i en maskin till en annan virtuell maskin som styrs av angriparen. En sådan kommunikationskanal är intressant att använda vid angrepp där offrets maskin har högre krav på sekretess och därmed inte ska kunna kommunicera direkt med det nätverk som angriparen sitter på. Mughal, Syed och A. Khan (2014) visar på en sidokanal där upplevd prestanda i lagringssystemet används som signalväg och bygger på att en virtuell maskin genom att läsa eller skriva stora datamängder kan påverka den läs- och skrivprestanda som en annan maskin får.

Ett motmedel som fungerar mot samtliga dessa angrepp är att undvika samlokalisering av virtuella maskiner, något som skulle medföra att en stor del den praktiska vinsten med virtualisering förloras. Vissa angrepp är relativt enkla att motverka, till exempel cacheattackerna mot AES-nycklarna ovan där det finns lämpliga motmedel att använda i implementationen av kryptoalgoritmen.

5.1.2 g2s: Guest-to-self

Angrepp från gästen mot sig själv kan genomföras om sårbarheter tillförs gästen genom virtualiseringsmjukvaran, exempelvis om användare i ett gästsystem kan nyttja en svaghet i virtualiseringsmiljön för att genomföra en eskalering av privilegier. Ett exempel på detta drabbade flera VMware-produkter där en sårbarhet i hur produkterna hanterade processorn i Virtual-8086-läge gav möjlighet för användare i gästerna att köra priviligierad kod[35].

5.1.3 h2s: Host OS-to-self

Angripare med begränsad åtkomst i en värd kan nyttja sårbarheter i värdens virtualiseringsfunktioner för att eskalera sina privilegier. Ett exempel på detta är en felaktighet i hur applikationen *vmware-mount* använde delade mjukvarubibliotek vilket gav användare möjlighet att eskalera privilegier eftersom denna applikation kördes med systemadministratörsprivilegier[36].

5.1.4 g2h: Guest-to-host OS

Angrepp från gäst till värd kan vara av flera typer, däribland denial-of-service (DoS), informationsläckage, exekvering av godtycklig kod samt modifiering av filer. En DoS-attack riktas primärt mot tillgängligheten i systemet medan de andra typerna av angrepp kan användas för att åstadkomma skada mot såväl tillgänglighet som riktighet och sekretess. Ett av de exempel som Pék, Buttyan och Bencsath (2013) tar upp är Cloudburst[37], där angripare kunde nyttja en sårbarhet som fanns i flera VMware-produkter för att exekvera godtycklig kod på värden.

35 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2267 [hämtat 2017-06-07]
36 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4296 [hämtat 2017-06-07]
37 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1244 [hämtat 2017-06-07]

5.1.5 g2hy: Guest-to-hypervisor

Denna typ av angrepp innebär att en gäst kan angripa värdens hypervisor direkt och därmed få möjlighet att köra godtycklig kod. Ett lyckat angrepp mot hypervisorn ger i princip oinskränkt inflytande över samtliga virtuella maskiner som körs på den drabbade fysiska maskinen. Ett exempel på ett sådant angrepp utnyttjade en sårbarhet i en drivrutin för ett nätverkskort för att exekvera kod i Xens hypervisor (Wojtczuk och Rutkowska 2011).

Wu, Wang och Jiang (2013) beskriver en metod att flytta stor del av funktionaliteten i den värdbaserade virtualiseringsmjukvaran KVM från den priviligerade minnesrymden, med höggradig tillgång till maskinen, till användarnas minnesrymd där mjukvaran endast får begränsad åtkomst till hårdvaran. På detta sätt har Wu, Wang och Jiang (2013) minskat mängden kod i priviligerade domänen från ungefär 33600 rader till 2300 rader, en minskning med mer än 93 %. Deras arbete visar tydligt att det finns utrymme för att optimera systemen när det gäller att minimera de möjliga angreppsytorna.

5.1.6 h2g: Host OS-to-guest

I fallet med systemvirtualisering av typ 2 har i regel värdoperativsystemet mycket stora befogenheter över gästerna, exempelvis genom att hantera deras virtuella hårddiskar och genom att hypervisorn körs som applikation under aktuell användare i värdoperativsystemet. I typ 1-virtualisering, där värdoperativsystemet körs i den virtualiserade miljön, är det däremot inte lika uppenbart att värden behöver ha åtkomst till gästerna. Rocha, Gross och Van Moorsel (2013) visar hur Xens Dom0 har omfattande tillgång till gästernas minnesutrymmen och hur detta kan användas för att angripa kritiska processer i gästerna. Rocha, Gross och Van Moorsel tar upp detta som ett säkerhetsmässigt designfel då Dom0 förvisso behöver ha tillgång till minnet i gästen, men att behovet är begränsat till vissa specifika och relativt små minnesområden.

5.1.7 h2hy: Host OS-to-hypervisor

På samma sätt som för h2g-angreppsytorna så är det en tydlig skillnad mellan virtualisering av typ 1 och typ 2 när det gäller angrepp från värdoperativsystemet till hypervisorn. Exempelvis körs VirtualBox, som är en typ 2-miljö, i normalfallet med samma privilegier som den inloggade användaren vilket också innebär att användaren har fullständig kontroll över hypervisorn och dess gäster.

I typ 1-virtualisering har värdoperativsystemet inte samma privilegier som för typ 2, och då krävs normalt sett ett angrepp för att ta över hypervisorn. Ett exempel på ett sådant angrepp presenterades av Wojtczuk (2008), där angripare i Xens administrativa domän Dom0 kunde nyttja en sårbarhet i hypervisorn för att exekvera godtycklig kod i denna. Angreppet byggde på en sårbarhet där DMA-överföringar via exempelvis nätverkskort användes för att få in exekverbar kod i hypervisorn.

Tabell 1: Nätverk i en virtualiserad miljö.

Nätverk	Användning
Management	Hantering av den virtuella miljön.
Migrering	Flyttning av virtuella maskiner mellan olika fysiska servrar.
Lagring	Åtkomst från fysiska/virtuella servrar till lagringssystemet.
Produktion	Kommunikation med systemets användare.

5.2 Nätverksangrepp

Den virtualiserade miljön måste betrakta samtliga nätverk som mer eller mindre obetrodda och skydda systemet därefter. Pék, Buttyan och Bencsath (2013) separerar diskussionen för nätverk utifrån fyra olika syften enligt tabell 1. Beroende på såväl säkerhetskraven som de tekniska kraven på systemet kan nätverken vara fysiskt åtskilda[38], logiskt åtskilda (till exempel genom VLAN) eller inte åtskilda alls.

Managementnätverket används av systemadministratörer för att hantera den virtuella miljön, till exempel skapa, starta och stänga av virtuella maskiner. Managementnätverket hanterar normalt sett endast metadata om gästerna till skillnad från migrations- och lagringsnätverken som direkt används för att överföra gästdata. Produktionsnätverket avser det nätverk där systemets klienter, till exempel användarterminaler, ansluter sig till de virtuella maskinerna. I kommersiella sammanhang är produktionsnätverket ofta kopplat mot Internet och exponeras därmed för de risker som detta medför.

5.2.1 Ökad angreppsyta för vanliga hot

De vanliga hoten mot nätverksanslutna maskiner finns kvar även i virtuella miljöer. Säkerhetsbrister i operativsystem och annan mjukvara som körs i de virtuella maskinerna kan utnyttjas för intrång och andra angrepp mot respektive virtuell maskin. Utöver de angrepp som kan genomföras i icke-virtualiserade miljöer så tillkommer de sårbarheter som tillförs till gästen genom virtualiseringsmiljön. Ett exempel på detta är en sårbarhet i VMware Tools[39] som gjorde att användare blev sårbara för malware[40].

Angripare med tillgång till lagringsnätverket har i princip samma möjligheter som i icke-virtualiserade miljöer. En försvårande faktor är att centraliserad lagring är vanligt i virtualiserade miljöer, vilket gör att angreppsytan finns i stor andel av de virtu-

[38] Fysiskt åskilda nätverk innebär att dessa använder separata nätverkskort, kablage och infrastrukturkomponenter. Inne i den fysiska servern är kommunikationen endast logiskt åtskild för samlokaliserade servrar.

[39] VMware Tools är ett applikations- och drivrutinspaket som kan köras i gäster under flera virtualiseringsprodukter från VMware. Paketet innehåller olika integrationsfunktioner som till exempel nätverks- och grafikdrivrutiner samt stöd för att använda mus.

[40] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1141 [hämtat 2017-06-07]

aliserade systemen. Lagringsnätverkens säkerhet är dock inget problem som är specifikt för virtualiserade miljöer.

En aspekt att ta hänsyn till är att traditionella, fysiska komponenter som används för att övervaka system mot angrepp, till exempel intrångsdetekteringssystem[41], inte går att använda i virtualiserade nätverk då en stor del av trafiken i regel stannar inom det virtuella nätverket och därmed inte når det fysiska nätverket. Detta utgör inget större problem gentemot externa angrepp, men om angrepp kan genomföras i det virtuella nätverket, till exempel från en virtuell maskin till en annan, så krävs nya typer av skyddsmekanismer (Jansen 2011). I dagsläget finns flera virtuella intrångsdetektorer på marknaden som går att integrera i virtualiserade miljöer, således har detta problem minskat i omfång.

5.2.2 Angrepp i migrationsnätverket

I de fall som migration av virtuella maskiner används så innebär migrationsnätverket en angreppsyta med en del specifika angrepp, där ett flertal bygger på att autentisering och riktighetsskydd ofta saknas eller är avslaget[42]. Exempelvis kan angripare med tillgång till migrationsnätverket avlyssna och manipulera överföringar av virtuella avbildningar för att komma åt känslig information och införa skadlig kod. Ett exempel på detta är Xensploit (Oberheide, Cooke och Jahanian 2008) som utför en man-in-the-middle-attack där minnesrymden för *sshd*-processen[43] i den virtuella maskinen manipuleras under migrering så att autentisering inte längre krävs för fjärrinloggning.

Om migreringsfunktionen tillåter migration av virtuella maskiner utan krav på autentisering av målmaskinen kan angripare med tillgång till migrationsnätverket ta över en virtuell maskin genom att begära att den migreras till en fysisk maskin som angriparen kontrollerar (Shetty, Anala och Shobha 2012). Angriparen kan sedan utföra ett stort spann av angrepp på den virtuella maskinen, till exempel manipulera minnesinnehåll, extrahera information och byta ut applikationer. När angreppet är avslutat kan maskinen migreras tillbaka till ordinarie hårdvara där den dessutom kan användas för att angripa hypervisorn och andra mål på den fysiska maskinen.

5.2.3 Angrepp på virtuella nätverkskomponenter

En funktion som tillkommer i virtualiserade miljöer är virtuella nätverkskomponenter. Dessa kan funktionellt motsvara exempelvis en Ethernet-switch men implementeras i mjukvara och körs under hypervisorn. De virtuella nätverkskomponenterna ut-

41 Eng. *intrusion detection system (IDS)*.

42 Bristfälligheten i skyddet av migrationstrafik visas exempelvis av att VMware introducerade skyddad migrering, med såväl kryptering som riktighetsskydd, först i vSphere 6.5 som släpptes 2016-10-18. Se https://blog.vmware.com/vsphere/2016/10/whats-new-in-vsphere-6-5-security.html [hämtat 2017-03-08].

43 sshd är den mjukvara som implementerar fjärrinloggning via protokollet Secure Shell (SSH) i många Linux-baserade operativsystem.

gör en angreppsyta mot systemet och kan innehålla sårbarheter i priviligerade systemdelar.

5.3 Övriga angrepp

Utöver interna angrepp och nätverksangrepp finns andra angreppsvägar som kan utnyttjas mot virtualiserade miljöer. Detta avsnitt beskriver några sådana angreppsvägar som även kan förekomma i icke-virtualiserade miljöer, men som sannolikt är vanligare eller kan ge större skador i virtualiserade miljöer.

5.3.1 Kloning av virtuella maskiner

Sårbarheter kan uppstå i virtualiserade miljöer där kloning från diskavbildningar[44] används för att förenkla installation, administration och backup av systemet. När flera maskiner skapas från samma avbildning finns risken att säkerhetsrelevanta tillstånd i maskinen återanvänds, till exempel för generering av slumptal.

Samma effekt kan fås om en ögonblicksbild tas av en maskin då även säkerhetsmässigt relevanta tillstånd sparas. Everspaugh m. fl. (2014) visar att slumptalsgenerering i Linux, FreeBSD och Windows är sårbar för denna typ av återanvändning av tillstånd, som då kan leda till att dålig slump används. Två olika typer av angrepp kan göras baserat på denna sårbarhet. I det första fallet utgår angreppet från att slumptillståndet återanvänds när en maskin återställs från en ögonblicksbild eller instansieras igen från en klon. Detta kan leda till återanvändning av kryptonycklar, initialvektorer och annan kryptologiskt relevant data vilket i sin tur kan utnyttjas i ett angrepp mot kryptofunktioner. Det andra fallet är att angriparen får tillgång till en klon eller ögonblicksbild så att denne själv kan köra slumpgenereringen i maskinen och därmed potentiellt kan få fram exakt samma slumptal som de som genereras av maskinen som ska angripas.

En diskavbildning innehåller ofta spår av tidigare aktiviteter i systemet i form av loggar, raderade filer och annan data. Balduzzi m. fl. (2012) genomförde en säkerhetsgenomgång av över 5000 färdiga publikt tillgängliga avbildningar för Amazon EC2[45]. I genomgången konstaterades att andelen avbildningar som innehöll mjukvara med kända sårbarheter var hög, med kritiska sårbarheter i 98 % av de Windows-baserade och 58 % av de Linux-baserade avbildningarna. Ungefär 22 % av avbildningarna innehöll publika SSH-nycklar som tillät avbildningens upphovsman att logga in. Det förekom även kvarglömd data, i form av såväl kvarlämnade som raderade men ej överskrivna filer. Kvarglömd data innehöll bland annat privata nycklar, lösenord, bilder och dokument.

---

44 En diskavbildning (eng. *disk image*) är typiskt en fil som innehåller en kopia av innehållet på en (fysisk eller virtuell) disk. En diskavbildning är generellt sett inte till för att användas direkt i en maskin utan ska snarare användas som säkerhetskopia eller för att kunna skapa en klon av en virtuell (eller fysisk) maskin baserat på diskens innehåll.

45 Amazon EC2 använder namnet AMI, *Amazon Machine Image*, för dessa färdiga avbildningar.

5.3.2 Återställningspunkter

En stor andel av virtualiseringsmjukvarorna innehåller funktioner för att skapa ögonblicksbilder av virtuella maskiner. I sådana ögonblicksbilder sparas det kompletta tillståndet för maskinen så att det senare går att återuppta exekveringen från exakt samma tillstånd. Ögonblicksbilder kan ses som ett specialfall av kloning, men där syftet är att skapa kopior på kända tillstånd hos maskinen, snarare än att skapa ytterligare maskiner med samma egenskaper. Typisk användning av ögonblicksbilder är säkerhetskopior för att kunna återställa ett tidigare tillstånd[46], exempelvis från en tidpunkt innan en maskin har angripits eller på något annat sätt gått sönder.

Ögonblicksbilder innebär samma säkerhetsproblematik som kloning när en virtuell maskin återställs (Ali, S. U. Khan och Vasilakos 2015). Förutom förlust av användardata som tillförts sedan ögonblicksbilden togs så kommer även andra ändringar som har gjorts att försvinna, exempelvis säkerhetsuppdateringar och ändringar i behörigheter. Detta kan leda till att återställningen återför maskinen till ett osäkert tillstånd. Ytterligare problem är återanvändning av kritiska tillstånd för exempelvis slumpgenerering, på samma sätt som kan ske vid kloning av maskiner.

5.3.3 Angrepp mot lagringsmedia

Om system använder delad lagringsmedia, det vill säga att flera virtuella maskiner lagrar sin information på samma fysiska hårddiskar, så kan det innebära ytterligare exponering av potentiellt känslig data. Exempelvis kan det bli svårt att destruera fysiska media om system tas ur drift om andra system är samlokaliserade på samma media. Återanvändning av lagringsmedia kan även innebära en möjlighet för systemet att återskapa information som tidigare lagrats på mediat av ett annat system om radering inte utförts på ett säkert sätt.

5.3.4 Fysiska angrepp

Angripare med fysisk åtkomst till en server kan utföra samma angrepp som på motsvarande icke-virtualiserad server. Exempelvis kan angripare nyttja tillgången för att lägga in skadlig kod i servern och extrahera information ur denna. Angrepp på fysiska värdmaskiner i virtualiserade miljöer kan ge potentiellt större skadeverkan då många virtuella maskiner kan drabbas genom ett enskilt angrepp.

[46] Återställning av tidigare tillstånd benämns ofta med den engelska termen *rollback*.

6 Diskussion

Systemvirtualisering är en beprövad och utbredd teknik för att bygga såväl stora datacenterlösningar som mindre installationer. Fördelarna med virtualisering är många, däribland förenklad administration och bättre utnyttjande av fysiska resurser än i icke-virtualiserade miljöer. Virtualisering innebär dock att ytterligare lager med mjukvara introduceras samtidigt som fler system kan dela hårdvara, något som i många fall kan leda till ökade IT-säkerhetsrisker i systemet.

Föregående kapitel visar att allvarliga sårbarheter förekommer i välanvända och välkända virtualiseringsmjukvaror. Då det inte finns någon avsikt att presentera en komplett lista i denna rapport så utgör de kända sårbarheter som tas upp endast en liten delmängd av den totala mängden. Syftet med urvalet är att visa bredden på kända sårbarheter och att ingen del av något virtualiseringssystem kan antas vara helt fri från sårbarheter. Det faktum att endast ett fåtal virtualiseringsmjukvaror berörs i föregående kapitel beror till stor del på att dessa mjukvaror tillsammans har en hög marknadsandel och att de därmed studerats mer ingående av säkerhetsforskare.

6.1 Effekten på IT-säkerheten

Perez-Botero, Szefer och Lee (2013) sammanställer och kategoriserar ett antal sårbarheter utifrån bland annat källa och mål för angrepp. Resultatet visar att över 50 % av de sårbarheter som studerats kan nyttjas av mjukvara i användarrymden[47] och att andelen stiger till över 82 % av sårbarheterna om även kärnrymden[48] räknas med[49]. Det har inte framkommit något som tyder på en signifikant förändring av sårbarheternas fördelning vilket gör det rimligt att anta att möjligheterna att hitta sårbarheter i olika delar av virtualiseringsmiljön är motsvarande även idag.

Historiskt sett har det förekommit sårbarheter som täcker in samtliga angreppsvägar som tagits upp i denna rapport. Då spridda sårbarheter kan kedjas samman vid angrepp leder det till slutsatsen att det – så länge inget annat visats – måste antas att det finns sårbarheter i virtualiseringsmiljön som tillåter ett lyckat angrepp mot en tjänst i systemet att eskaleras till ett fullskaligt angrepp på systemet.

Det finns ett antal olika orsaker till sårbarheterna, där vissa har uppstått på grund av enkla programmeringsfel, till exempel att gränserna på en minnesbuffert inte hante-

47 Eng. *user space* eller *application space*, det vill säga minne som inte är priviligerat i systemet.

48 Eng. *kernel space*, priviligerat minnesutrymme i systemet.

49 Perez-Botero, Szefer och Lee (2013), tabell 2, summering av raderna ”Network” och ”Guest VM User Space” respektive raderna ”Network”, ”Guest VM User Space” och ”Guest VM Kernel Space”.

ras korrekt[50], medan andra brister beror på komplexa beroenden mellan mjukvara och hårdvara. I det senare fallet är interaktionen oftast så komplex att det i praktiken varit omöjligt att genomföra en heltäckande testning av systemet.

Virtualisering innebär alltid att en mängd mjukvara tillförs i systemet för att separera gästerna och för att ge ett lämpligt hårdvarulikt gränssnitt mot de virtuella maskinerna. Även om denna mjukvara tas fram med strikta metoder för att säkerställa kvaliteten så finns risken att den innehåller kritiska sårbarheter som äventyrar IT-säkerheten i systemet. Genom lämpliga utvecklingsmetoder och härdning av systemen kan riskerna minimeras, men i praktiken går de inte att eliminera helt.

En slutsats är att virtualisering i allmänhet sänker IT-säkerhetsnivån sett ur ett rent tekniskt perspektiv. Den sammantagna, faktiska effekten på säkerhetsnivån måste dock bedömas för varje specifikt IT-system och användningsfall, då det är möjligt att de positiva effekterna överväger. När virtualiseringsteknik används tillkommer angreppsytor och därmed risker som måste hanteras.

6.2 Separation genom virtualiseringsteknik

Om fysiska maskiner byts ut mot samlokaliserade virtuella maskiner så byts även den fysiska separationen mellan maskinerna ut mot en logisk, mjukvarubaserad separation. Detta innebär en större exponering mellan maskinerna och att separationen blir svagare än i motsvarande fysiskt uppdelade system.

En viktig aspekt att ta hänsyn till vid säkerhetsanalysen är om virtualiseringstekniken verkligen används för separation i det aktuella systemet. Virtualiseringen kan även användas för att nå en funktionell uppdelning inom en informationsdomän, med avsikt att förenkla utveckling, drift och underhåll av systemet. I dessa fall kan virtualisering vara godtagbar, givet att uppdelningen gjorts på ett lämpligt sätt och att vissa kritiska funktioner hanteras korrekt, exempelvis logghantering.

Att använda virtualisering för att upprätthålla separation mellan informationszoner eller informationssäkerhetsklasser är problematiskt då hypervisorn i dessa fall utgör den säkerhetskomponent som implementerar separationen. Separationen är ett av de områden där det ställs speciellt höga krav på säkerhet då den utgör en skyddsbarriär som ska förhindra såväl intrång som läckage.

Informationsläckage behöver inte vara en följdeffekt utav angrepp, utan kan även inträffa som effekt av felaktig funktion. Den felaktiga funktionen kan uppstå av olika orsaker, exempelvis genom programmeringsfel, trasig hårdvara och spontana enkelfel[51] i minne och processortillstånd. Den senare typen av fel beaktas normalt sett in-

[50] Denna typ av brist kan benämnas med ”buffertspill” eller ”buffertöverskridning” på svenska men oftast används de engelska termerna *buffer overflow* och *buffer overrun* även i svenskspråkig text. Samtliga varianter är synonyma.

[51] Spontana enkelfel orsakas av slumpmässiga fenomen, typiskt i form av naturligt förekommande joniserande strålning. De spontana enkelfelen kan påverka information som lagras i datorminnen,

te i systemen men är relevant i vissa fall där separationen ska hantera hög informationssäkerhetsklass.

Separationen i virtualiserade system upprätthålls av flera komponenter som måste samverka och fungera korrekt, exempelvis hypervisor-mjukvara och hårdvara i form av processor och chipset. Samtliga dessa komponenter är felkritiska systemdelar då felaktig funktion i någon av dessa komponenter kan leda till att separationen fallerar.

6.3 MUST:s riktlinjer

Utöver de allmänna kraven på säkerhetsfunktioner som anges i *KSF 3.1* (Försvarsmakten 2014) så har MUST gett ut specifika riktlinjer kring användning av virtualiseringsteknik i IT-system (Försvarsmakten 2016). Dessa riktlinjer pekar på ett antal funktioner som måste separeras fysiskt för att undvika sammanblandning och olämplig exponering av information, exempelvis loggning, behörighetsdatabaser och nätverkstrafik.

Utifrån kraven i KSF 3.1 kan det tänkas vara acceptabelt med separation genom virtualiseringsmiljön för vissa system som hanterar information i lägre informationssäkerhetsklasser under förutsättning att tillräcklig kunskap och tilltro kan sättas till den specifika virtualiseringsmjukvaran[52]. I MUST:s riktlinjer står det uttryckligen att hypervisorer inte uppfyller de krav som ställs på en separationsmekansim mellan informationssäkerhetsklasser, signalskyddsdomäner och säkerhetsdomäner.

Enligt såväl MUST:s riktlinjer om virtualisering samt KSF 3.1 är virtualiseringstekniken inte lämpad att upprätthålla separation mellan kritiska system. Detta stämmer väl överens med resultaten i denna rapport, där IT-säkerhetsriskerna på grund av allvarliga sårbarheter i miljön påvisas. Slutsatsen av detta är att virtualiseringstekniken kräver stor försiktighet och att noggranna riskanalyser genomförs innan tekniken används i kritiska system.

6.4 Slutsatser

Även inom Försvarsmaktens IT-system är virtualisering en värdefull teknik som kan nyttjas för att nå verksamhets- och driftfördelar så länge riskerna är hanterliga. En viktig aspekt att ta hänsyn till vid riskbedömningen är virtualiseringens roll i systemet, exempelvis om den ska upprätthålla separation mellan informationsdomäner eller om tekniken nyttjas för att nå driftfördelar inom en och samma informationsdomän.

---

exempelvis minne som innehåller instruktioner som styr funktionen i hypervisorn. Denna typ av fel benämns ofta med engelskans *single-event upset*.

52 Enligt resonemanget i KSF 3.1 måste hypervisorn anses utgöra en säkerhetskomponent som upprätthåller separationen. Om samtliga system i den virtuella miljön behandlar information på samma informationssäkerhetsklass kan KSF-reglerna möjligtvis tillåta att systemet hanterar information på nivån *Hemlig/Restricted* under rätt förutsättningar. I vissa specialfall kan det eventuellt även vara möjligt på nivån *Hemlig/Confidential*. Däremot är det inte givet att kraven på hypervisorn som separationsfunktion kan uppfyllas om informationssäkerhetsklasser blandas, ens då *Hemlig/Restricted* utgör den högsta informationssäkerhetsklassen som hanteras i miljön.

Risken för att såväl misstag som angrepp ska få mer utbredda konsekvenser är i regel större i virtualiserade miljöer än i miljöer byggda på fysiskt åtskilda maskiner. I vissa fall är det tänkbart att risken är acceptabel sett utifrån de fördelar som virtualiseringen innebär. I andra fall, till exempel om virtualiseringen måste upprätthålla en separation som ska skydda information med hög informationssäkerhetsklass, så är risken sannolikt för hög med tillgängliga virtualiseringstekniker. Införandet av virtualisering i kritiska IT-system måste därmed föregås av noggranna riskbedömningar, med fokus på områden där säkerheten blir beroende av virtualiseringsmiljön, för att säkerställa att en lämplig risknivå kan upprätthållas.

Litteratur

Ali, M., S. U. Khan och A. V. Vasilakos (2015). ”Security in cloud computing: Opportunities and challenges”. I: *Information Sciences* 305, s. 357–383. DOI: 10.1016/j.ins.2015.01.025.

Balduzzi, M., J. Zaddach, D. Balzarotti, E. Kirda och S. Loureiro (2012). ”A Security Analysis of Amazon’s Elastic Compute Cloud Service”. I: *Proc. of the 27th Annual ACM Symposium on Applied Computing (SAC)*.

Bengtsson, A. och L. Westerdahl (2009). *Virtual Machines - Security Qualities*. Tekn. rapport FOI-R--2904--SE. FOI, Totalförsvarets Forskningsinstitut.

Brohi, S. N., M. A. Bamiah, M. N. Brohi och R. Kamran (2012). ”Identifying and analyzing security threats to virtualized cloud computing infrastructures”. I: *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management, ICCCTAM 2012*, s. 151–155. DOI: 10.1109/ICCCTAM.2012.6488089.

Chiang, R. C., S. Rajasekaran, N. Zhang och H. H. Huang (2015). ”Swiper: Exploiting virtual machine vulnerability in third-party clouds with competition for I/O resources”. I: *IEEE Transactions on Parallel and Distributed Systems* 26.6, s. 1732–1742. DOI: 10.1109/TPDS.2014.2325564.

Everspaugh, A., Y. Zhai, R. Jellinek, T. Ristenpart och M. Swift (2014). ”Not-So-Random numbers in virtualized Linux and the Whirlwind RNG”. I: *Proceedings - IEEE Symposium on Security and Privacy*, s. 559–574. DOI: 10.1109/SP.2014.42.

Försvarsmakten (2014). *KSF, Krav på IT-säkerhetsförmågor hos IT-system, v3.1*.

– (2016). *Riktlinjer, säkerhetskrav och villkor för virtualisering*.

Hashizume, K., D. G. Rosado, E. Fernández-Medina och E. B. Fernandez (2013). ”An analysis of security issues for cloud computing”. I: *Journal of Internet Services and Applications* 4.1, s. 1–13. DOI: 10.1186/1869-0238-4-5.

Hörmanseder, R. och M. Jäger (2014). ”Cloud security problems caused by virtualization technology vulnerabilities and their prevention”. I: *IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks*, s. 373–383.

Huang, Y.-L., B. Chen, M.-W. Shih och C.-Y. Lai (2012). ”Security impacts of virtualization on a network testbed”. I: *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability, SERE 2012*, s. 71–77. DOI: 10.1109/SERE.2012.17.

Irazoqui, G., M. S. Inci, T. Eisenbarth och B. Sunar (2014). ”Wait a minute! A fast, cross-VM attack on AES”. I: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8688 LNCS, s. 299–319. DOI: 10.1007/978-3-319-11379-1_15.

– (2015). ”Fine grain Cross-VM attacks on Xen and VMware”. I: *Proceedings - 4th IEEE International Conference on Big Data and Cloud Computing, BDCloud 2014 with the 7th IEEE International Conference on Social Computing and Networking, Soci-*

alCom 2014 and the 4th International Conference on Sustainable Computing and Communications, SustainCom 2014, s. 737–744. DOI: 10.1109/BDCloud.2014.102.

Jansen, W. A. (2011). ”Cloud Hooks: Security and Privacy Issues in Cloud Computing”. I: *Proc. of the 44th Hawaii International Conference on System Sciences*.

Karlzén, H. (2012). *Molnet - möjligheter och begränsningar*. Tekn. rapport FOI-R--3381--SE. FOI, Totalförsvarets Forskningsinstitut.

Kaspersky (u.å.). *Security for virtualization: Finding the right balance*. Tekn. rapport. Kaspersky Lab. URL: http://www.kaspersky.co.uk/downloads/pdf/virtualization.pdf.

Mughal, B. K., A. Syed och A. Khan (2014). ”Information leakage in the cloud”. I: *ICOSST 2014 - 2014 International Conference on Open Source Systems and Technologies, Proceedings*, s. 56–61. DOI: 10.1109/ICOSST.2014.7029320.

Oberheide, J., E. Cooke och F. Jahanian (2008). ”Empirical exploitation of live virtual machine migration”. I: *Proc. of BlackHat DC convention*.

Ormandy, T. (2007). *An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments*. Tekn. rapport. Google, Inc.

Parker, D. B. (2014). ”Toward a New Framework for Information Security”. I: *The Computer Security Handbook*. Utg. av S. Bosworth, M. E. Kabay och E. Whyne. sjätte. New York, NY, USA: John Wiley & Sons, Inc. ISBN: 978-1-118-12706-3.

PCI (2011). *PCI DSS 2.0, Information Supplement: PCI DSS Virtualization Guidelines*. Tekn. rapport. PCI. URL: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

Pék, G., L. Buttyan och B. Bencsath (2013). ”A survey of security issues in hardware virtualization”. I: *ACM Computing Surveys* 45.3. DOI: 10.1145/2480741.2480757.

Perez-Botero, D., J. Szefer och R. B. Lee (2013). ”Characterizing hypervisor vulnerabilities in cloud computing servers”. I: *Cloud Computing 2013 - Proceedings of the 2013 International Workshop on Security in Cloud Computing*, s. 3–10. DOI: 10.1145/2484402.2484406.

Ristenpart, T., E. Tromer, H. Shacham och S. Savage (2009). ”Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds”. I: *Proceedings of the ACM Conference on Computer and Communications Security*, s. 199–212. DOI: 10.1145/1653662.1653687.

Rocha, F., T. Gross och A. Van Moorsel (2013). ”Defense-in-depth against malicious insiders in the cloud”. I: *Proceedings of the IEEE International Conference on Cloud Engineering, IC2E 2013*, s. 88–97. DOI: 10.1109/IC2E.2013.20.

Shetty, J., M. R. Anala och G. Shobha (febr. 2012). ”A Survey on Techniques of Secure Live Migration of Virtual Machine”. I: *International Journal of Computer Applications* 39.12, s. 34–39. DOI: 10.5120/4875-7305.

Symantec (2012). *The Virtual Telco: Security & High Availability Are Key to Virtualization Advantage*. Tekn. rapport. Symantec. URL: https://www.symantec.com/content/en/us/enterprise/white_papers/b-HR-Symantec-Virtualization-WP.pdf.

Wojtczuk, R. (2008). ”Xen 0wning Trilogy: Part 1”. I: *Proc. of BlackHat USA convention*. URL: http://invisiblethingslab.com/resources/bh08/part1.pdf.

Wojtczuk, R. och J. Rutkowska (2011). *Following the White Rabbit: Software attacks against Intel VT-d technology*. Tekn. rapport. URL: http://invisiblethingslab.com/resources/2011/Software%20Attacks%20on%20Intel%20VT-d.pdf.

Wu, C., Z. Wang och X. Jiang (2013). ”Taming Hosted Hypervisors with (Mostly) Deprivileged Execution”. I: *Proc. of the 20th Annual Network and Distributed System Security Symposium, NDSS*.

Zhou, F., M. Goel, P. Desnoyers och R. Sundaram (2013). ”Scheduler vulnerabilities and coordinated attacks in cloud computing”. I: *Journal of Computer Security* 21.4, s. 533–539. DOI: 10.3233/JCS-130474.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se