Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Virtualiseer met verstand

Zorg dat u de buren van uw gevoelige virtuele systemen kent

Factsheet FS-2016-05 | versie 1.0 | 10 augustus 2016

Virtualisatie van ICT-diensten zorgt voor efficiënter en flexibeler gebruik van hardware. Deze factsheet gaat over specifieke risico's die ontstaan wanneer u virtuele servers gebruikt om ICT-diensten uit te besteden. Uw virtuele server heeft op de host een onbekend aantal virtuele buren. Met behulp van de nieuw ontdekte Flip Feng Shui-aanvalstechniek kan een aanvaller een virtuele buur binnendringen of malware laten installeren. Tot op heden kon een aanvaller activiteit van virtuele buren alleen afluisteren. De kans van slagen van zo'n aanval was veel kleiner. Het NCSC adviseert om in regels over informatiebeveiliging vast te leggen welke typen systemen er binnen uw organisatie voor virtualisatie in aanmerking komen. Leg daarbij ook vast in welk type cloud deze typen systemen mogen worden ondergebracht.

Achtergrond

Virtualisatie van ICT-diensten zorgt voor efficiënter en flexibeler gebruik van hardware. De meeste ICT-systemen maken lang niet altijd volledig gebruik van de beschikbare processorkracht, geheugen, schijfruimte en bandbreedte. Door meerdere ICT-systemen de hardware van een fysieke computer te laten delen, wordt deze hardware een groter deel van de tijd benut. Deze praktijk wordt (hardware)virtualisatie genoemd.

Een bekend voorbeeld van virtualisatie is het huren van een 'virtual private server' (VPS). Aanbieders variëren van kleinschalige ICT-bedrijven tot wereldwijde spelers als Amazon EC2 en Microsoft Azure.

Samenwerkingspartners

Team High-Tech Crime
Onderzoeksteam 'Flip Feng Shui'[1]
Belastingdienst
Atos

Doelgroep

Informatiebeveiligers, beheerders en architecten van organisaties die gevirtualiseerde diensten (zoals cloudservers) afnemen of intern gebruiken.

[1] Kaveh Razavi, Ben Gras en Erik Bosman, Vrije Universiteit Amsterdam; Bart Preneel, Katholieke Universiteit Leuven; Cristiano Giuffrida en Herbert Bos, Vrije Universiteit Amsterdam.

Een virtuele server is ondergebracht op een ***host***. Dat is het fysieke systeem waarop de virtuele server draait. De host wordt beheerd door de aanbieder die u de virtuele server levert. Uw virtuele server heeft op de host een meestal onbekend aantal virtuele buren. Dit zijn de virtuele servers van andere klanten van de aanbieder. Aanbieders brengen de virtuele servers onder op een groep hosts, een zogenaamde cloud. Er zijn verschillende typen clouds, die verschillen in de mate waarin virtuele servers van verschillende klanten op dezelfde host onder worden gebracht. Zie het kader 'Clouds: public, community en private' voor meer details.

De ***hypervisor*** is de software op de host die de verschillende virtuele servers toegang geeft tot de gedeelde hardware van de host. Bekende hypervisors op servers zijn bijvoorbeeld KVM, VMware ESXi en Xen.

Virtualisatie wordt ook op clientsystemen gebruikt. Bekende hypervisors op clientsystemen zijn bijvoorbeeld Oracle VirtualBox en VMware Workstation. De technische observaties in deze factsheet zijn ook daar van toepassing. Het handelingsperspectief is echter toegespitst op servertoepassingen.

Deze factsheet gaat over specifieke risico's die ontstaan wanneer u virtuele servers gebruikt om ICT-diensten uit te besteden. Daarnaast kent elk gebruik van clouddienstverlening ook algemene risico's. Als u virtuele servers gebruikt, zijn deze risico's ook van toepassing. Deze komen ter sprake in het NCSC-whitepaper Cloud Computing.[2] Deze factsheet vormt een aanvulling op de adviezen uit het whitepaper.

Clouds: public, community en private

Een aanvaller kan aanvallen via Flip Feng Shui of side channels pas uitvoeren als zijn virtuele server op dezelfde host draait als zijn slachtoffer. Hoe eenvoudiger een virtuele server op de host van uw virtuele server te verkrijgen is, hoe eenvoudiger een aanvaller een poging kan wagen binnen te komen.

In het NCSC-whitepaper Cloud Computing komen verschillende typen clouds aan bod. Deze verschillen in het gemak waarmee een buitenstaander een virtuele server kan verkrijgen op een van de hosts.

Een ***publieke cloud*** is voor iedereen toegankelijk. Iedereen die betaalt, krijgt de beschikking over een virtuele server op een van de hosts.

Een ***community cloud*** is voor een selecte groep toegankelijk. Het selectiemechanisme verschilt tussen aanbieders. Een voorbeeld is een aanbieder die een klantacceptatieprocedure hanteert.

Een ***private cloud*** is slechts voor één organisatie toegankelijk. Deze kan de cloud zelf hosten of onderbrengen bij een externe leverancier.

Wat is er aan de hand?

Aanvallers zijn in staat om gegevens aan te passen van servers die hun virtuele buren zijn. Daardoor zijn ze in staat op deze servers binnen te dringen of deze malware te laten installeren.

De Flip Feng Shui-aanvalstechniek (zie kader) is het eerste voorbeeld van een aanvalstechniek die een aanvaller in staat stelt wijzigingen in het geheugen van een andere virtuele server aan te brengen. Zo kan hij de virtuele server direct aanvallen.

Flip Feng Shui is niet slechts een theoretische kwetsbaarheid. Een aanvaller kan Flip Feng Shui in realistische omstandigheden, op een host met tientallen virtuele servers, toepassen. Wel is een gerichte aanval lastig. Het is niet eenvoudig om een virtuele server te verkrijgen die op dezelfde host draait als een bepaalde andere virtuele server. De kans van slagen van Flip Feng Shui hangt daarom sterk af van het type cloud waarin de virtuele server onder is gebracht.

Academici en andere onderzoekers vinden al jaren regelmatig manieren om vanuit een virtuele server zijn virtuele buren af te luisteren. Een manier om virtuele buren af te luisteren heet een ***side channel***,[3] omdat het gaat om een onbedoeld communicatiekanaal.

Wanneer een aanvaller zijn virtuele buren af kan luisteren, kan hij de beschikking krijgen over vertrouwelijke informatie die wordt verwerkt op de andere servers. Meestal lekken side channels maar een beperkte hoeveelheid informatie. De meeste aandacht gaat daarom uit naar het afluisteren van cryptografische sleutels. Dit zijn immers kleine stukjes informatie die desondanks cruciaal zijn voor de beveiliging van gegevens. Met een afgeluisterde cryptografische sleutel kan de aanvaller versleutelde gegevensdragers of onderschept netwerkverkeer ontsleutelen.

Side channels zijn niet eenvoudig in de praktijk te misbruiken. De meeste bekende side channels zijn slechts in een laboratoriumomgeving succesvol toegepast. In de praktijk bevat een host namelijk tientallen virtuele servers. Een aanvaller kan de signalen van zijn doelwit dan niet of nauwelijks onderscheiden van die van de andere servers. Ook is het voor de meeste aanvallers niet eenvoudig om af te dwingen dat hun virtuele server op dezelfde host draait als hun slachtoffer.

[2] Zie https://www.ncsc.nl/actueel/whitepapers/whitepaper-cloudcomputing.html.
[3] Side channels komen op meer plaatsen voor dan alleen tussen virtuele servers. Ook tussen twee processen op hetzelfde systeem kunnen bijvoorbeeld side channels bestaan.

De Flip Feng Shui-aanvalstechniek: vraag en antwoord

Hoe werkt de Flip Feng Shui-aanvalstechniek op hoofdlijnen?	Een aanvaller huurt een virtuele server op dezelfde host als uw virtuele server. De aanvaller verleidt de hypervisor er vervolgens toe om een bepaald stuk geheugen dat uw server en de zijne gemeen hebben, te ontdubbelen. Dat betekent dat beide systemen bepaalde informatie die ze allebei verwerken, in het zelfde deel van het fysieke geheugen opslaan. Met behulp van de zogenaamde rowhammer-techniek[4] is de aanvaller in staat de informatie in dit geheugen te veranderen zonder dat de hypervisor of uw virtuele server dit merkt. Hierdoor is hij in staat uw virtuele server te bewegen tot het installeren van malware of het toestaan van logins door ongeautoriseerde personen.
Welke systemen zijn kwetsbaar?	Alle virtuele servers die zijn ondergebracht op hosts die geheugenontdubbeling (memory deduplication) toepassen.
Ik ben eigenaar van een virtuele server: hoe kan ik de kwetsbaarheid wegnemen?	U kunt de kwetsbaarheid niet zelf wegnemen. Dring er bij de aanbieder van uw virtuele server op aan dat hij geheugenontdubbeling (memory deduplication) uitschakelt op de host waarop uw virtuele server ondergebracht is.
Hoe waarschijnlijk is het dat ik met de aanvalstechniek te maken krijg?	De onderzoekers hebben de code die ze hebben geschreven om misbruik van de kwetsbaarheid te maken, niet gepubliceerd. Voor een aanvaller met weinig kennis en middelen is de aanval daarom lastig uit te voeren. Voor een aanvaller met ruime kennis en middelen is de informatie in het onderzoeksrapport voldoende om de aanval uit te kunnen voeren. Een criminele organisatie of buitenlandse inlichtingendienst is hier waarschijnlijk goed toe in staat. Daarbij geldt echter wel dat hij zijn aanvalscode zal moeten aanpassen voor het specifieke besturingssysteem dat u op uw virtuele server gebruikt.
Hoe is de aanvaller in staat de virtuele server binnen te dringen?	In het onderzoeksrapport beschrijven de auteurs twee aanvallen op Debian en Ubuntu als voorbeeld. Met de eerste van deze aanvallen weet een aanvaller binnen te dringen in een server. De aanvaller richt zich op het aanpassen van een instelling van OpenSSH. Hij maakt een kleine wijziging in een publieke sleutel die is geautoriseerd om op de server in te loggen. Door deze wijziging kan hij de sleutel eenvoudig kraken. Zo verschaft hij zich toegang tot de server.
Hoe is de aanvaller in staat de virtuele server malware te laten installeren?	In het onderzoeksrapport beschrijven de auteurs twee aanvallen op Debian en Ubuntu als voorbeeld. Met de tweede van deze aanvallen weet een aanvaller de server malware te laten installeren. De aanvaller richt zich op het aanpassen van instellingen van softwarebeheerapplicatie apt. Hij brengt kleine wijzigingen aan in de URL waarvandaan apt software downloadt. Zo zorgt hij dat de server malware installeert die zich voordoet als een softwareupdate. Hij omzeilt de integriteitscontrole door ook een kleine wijziging te maken in de publieke PGP-sleutel waarmee apt de software controleert.
Wat maakt deze aanvalstechniek anders dan andere soortgelijke technieken?	Eerder ontdekte aanvalstechnieken, zogenaamde side channels, richten zich op het afluisteren van vertrouwelijke gegevens van een virtuele server op dezelfde host. Dit is de eerste aanvalstechniek die een aanvaller in staat stelt wijzigingen in het geheugen van een andere virtuele server aan te brengen. Zo kan hij de virtuele server direct aanvallen.
Waarom heet de aanvalstechniek Flip Feng Shui?	De naam van de aanvalstechniek valt in twee delen uiteen. ‘Flip’ slaat op de bitflips die de aanvaller weet te bewerkstelligen op uw virtuele server. ‘Feng Shui’ is een Chinese filosofie over het in overeenstemming brengen van zaken met hun omgeving. De manier waarop virtuele servers bij deze aanval wijzigingen van hun buren overnemen, doet hier sterk aan denken.
Waar kan ik meer informatie vinden over de aanvalstechniek?	De onderzoekers hebben hun resultaten gepresenteerd op het USENIX Security Symposium 2016. Hun slides en onderzoeksrapport zijn beschikbaar op https://www.vusec.net/projects/flip-feng-shui/.
Ik heb een andere vraag.	Een uitgebreide variant van deze ‘vraag en antwoord’, inclusief handelingsperspectief voor eigenaren van hosts, staat op https://www.ncsc.nl/actueel/factsheets/flip-feng-shui-aanvalstechniek-vraag-en-antwoord.html.

[4] Zie bijvoorbeeld https://en.wikipedia.org/wiki/Row_hammer.

Handelingsperspectief

1. Voer een risicoanalyse uit om voor elk type ICT-systeem van uw organisatie te bepalen of dit wel of niet gevirtualiseerd mag worden. Leg daarbij ook vast in welk type cloud deze typen systemen mogen worden ondergebracht. Dit kunt u afleiden uit de gevoeligheid van de processen waar het deel van uitmaakt.
2. Vraag uw aanbieder in welke typen cloud hij uw virtuele servers kan onderbrengen. Vraag welke toelatingscriteria er gelden voor private en community clouds.
3. Leg uw keuze vast in regels over informatiebeveiliging, inclusief de onderliggende overwegingen.
4. Migreer virtuele ICT-systemen die niet in het juiste type cloud draaien, naar een niet-gevirtualiseerde omgeving of een private of community cloud.

Wat kan er gebeuren?

Als u een virtuele server gebruikt, kan een virtuele buur gegevens in het geheugen van uw server wijzigen. Zo kan hij in uw virtuele server inbreken. Ook kan hij uw server opdracht geven om malware te downloaden en te installeren. Dit kan hij doen met de Flip Feng Shui-aanvalstechniek (zie kader). Het valt te verwachten dat er in de toekomst meer van dergelijke aanvalstechnieken gevonden zullen worden. Flip Feng Shui is ook uit te voeren als er vele andere virtuele servers op de host aanwezig zijn. Wel moet de aanvaller afdwingen dat zijn virtuele server op dezelfde host draait als zijn doelwit. Bij een ongerichte aanval is dit laatste natuurlijk niet van toepassing.

Naast Flip Feng Shui, bestaan er al langer aanvalstechnieken waarmee virtuele servers hun virtuele buren kunnen afluisteren. De kans hierop is echter veel kleiner. Los van de opgave om een virtuele server op dezelfde host als het slachtoffer te draaien, is het afluisteren van één virtuele server tussen tientallen anderen bepaald niet eenvoudig. De kans hierop is dan ook klein. Voor de meeste virtuele servers zijn algemene cloudrisico's veel groter, zoals het risico dat uw aanbieder of een derde partij via de hypervisor toegang krijgt tot uw gegevens.

Elke aanval in deze categorie is alleen mogelijk zo lang de eigenaar van de host nog niet de juiste update heeft geïnstalleerd of de juiste instelling heeft gedaan. In het algemeen brengen leveranciers van hypervisors updates of instructies uit om nieuw ontdekte aanvalstechnieken te voorkomen. Als klant kunt u echter niet zelf vaststellen of uw aanbieder deze maatregelen al heeft getroffen.

Wat adviseert het NCSC?

Het NCSC adviseert om in regels over informatiebeveiliging vast te leggen welke typen systemen er binnen uw organisatie voor virtualisatie in aanmerking komen. Leg daarbij ook vast in welk type cloud deze typen systemen mogen worden ondergebracht. Deze regels moeten worden toegepast bij de aanschaf en beveiliging van ICT-systemen. Om welke systemen het gaat, bepaalt u op basis van een risicoanalyse. U kunt bijvoorbeeld besluiten dat u de risico's van aanvalstechnieken als Flip Feng Shui en side channels in een publieke cloud voor bepaalde categorieën systemen acceptabel vindt. Deze conclusie is bijvoorbeeld gerechtvaardigd als deze systemen nauwelijks gevoelige gegevens verwerken.

Alleen als een aanvaller in staat is om uw virtuele buur te worden, kan hij aanvallen via side channels of Flip Feng Shui uitvoeren. Deze aanvallen werken dus niet als de aanvaller geen toegang heeft tot virtuele servers op de zelfde host. Dit kunt u bijvoorbeeld adwingen door te zorgen dat alleen uw organisatie virtuele servers op deze host heeft ondergebracht en dat aanvallers de andere servers ook niet weten binnen te dringen. Vraag uw aanbieder welke toelatingscriteria hij hanteert bij het toelaten van virtuele servers op de hosts waar uw virtuele servers zijn ondergebracht.

Pas uw aangepaste regels voor virtualisatie van ICT-systemen ook toe op al bestaande virtuele servers. Migreer ICT-systemen naar cloudomgevingen van het juiste type. Migreer naar niet-virtuele servers als uw regels over informatiebeveiliging stellen dat deze systemen niet gevirtualiseerd mogen worden.

Tot slot

Flip Feng Shui is een significante verandering van het risicoprofiel van virtuele servers. Sidechannelaanvallen waren vooral een theoretisch risico. Dat geldt niet voor Flip Feng Shui. Aanbieders kunnen maatregelen treffen om de techniek zelf tegen te gaan. Het valt te verwachten dat onderzoekers in de komende jaren vaker dit soort aanvalstechnieken zullen ontdekken. Het is daarom belangrijk dat uw aanbieder up-to-date is over de recentste ontwikkelingen.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-05 | versie 1.0 | 10 augustus 2016