Een heerlijke nieuwe beveiligingswereld

Een heerlijke nieuwe beveiligingswereld

hoe beveiliging verandert om virtualisering en cloud computing te ondersteunen

Technisch verslag van Trend Micro™ | januari 2011

Door Eva Chen

EEN HEERLIJKE NIEUWE BEVEILIGINGSWERELD: HOE BEVEILIGING VERANDERT OM VIRTUALISERING EN CLOUD COMPUTING TE ONDERSTEUNEN

I. SAMENVATTING EN TOELICHTING

De verwachting is dat alle aspecten van informatietechnologie in de nabije toekomst verplaatsbaar, dynamisch en interactief zullen zijn: de toegang, de gegevens, de werklast en alle computer-activiteiten. Gebruikers zullen met mobiele apparaten honderden gigabytes aan gegevens kunnen openen en opslaan. Virtuele servers zullen computervermogen mobiliseren tussen netwerksegmenten en datacenters, maar zullen dat ook buiten de ondernemingsomgeving en de openbare cloud inbrengen, waar computervermogen zal worden aangeboden als een nutsvoorziening.

Als gevolg van deze grote veranderingen zullen alle aspecten van informatiebeveiliging opnieuw tegen het licht moeten worden gehouden. In de traditionele netwerkbeveiliging werd computer-vermogen (machines, gegevensopslag e.d.) als een bewaakte, ommuurde tuin gezien. Dat kan straks niet meer. Er is een nieuwe generatie beveiligingspraktijken ontstaan, waarbij de nadruk ligt op de dynamische kant van computervermogen en gegevens.

Deze revolutionaire veranderingen vinden echter niet van de ene dag op de andere plaats. De belangrijkste vraag voor ondernemingen is hoe ze van hun huidige situatie, via een overgangsperiode of een hybride fase, de overstap naar de nieuwe situatie kunnen maken. Er is niet één universeel antwoord: elke organisatie doet dit in een eigen tempo, dat zal afhangen van de gestelde eisen en andere bepalende factoren. Oplossingen moeten dus flexibel zijn en met deze diversiteit rekening houden. In dit technisch verslag wordt beschreven hoe deze veranderingen evolueren bij de overstap naar virtualisering en vervolgens cloud computing. Vervolgens wordt beschreven hoe Trend Micro de evolutie van beveiliging ziet als de sleutel tot mobiliteit, virtualisering en cloud computing.

II. INLEIDING

Volgens analisten is de wereldwijde netwerkbeveiligingsmarkt in 2009 gegroeid tot meer dan 7 miljard dollar en is de beveiligingsmarkt voor hosts/endpoints binnen ondernemingen gegroeid tot meer dan 2 miljard dollar. Waarom zouden de verhoudingen tussen deze uitgaven in de toekomst wel eens andersom kunnen liggen? Omdat de markt voor traditionele netwerkbeveiliging kleiner wordt naar-mate netwerken minder relevant worden door de dynamische verplaatsing van computervermogen en gegevens. De markt voor beveiliging van hosts, waar het host voor het computervermogen en de gegevens zelf worden beschermd, zal juist sterk groeien; de dynamische host moet zelf het primaire punt van bescherming worden.

De omvang en reikwijdte van de veranderingen in de informatietechnologie en -beveiliging is zonder meer indrukwekkend. Stel dat Butch Cassidy en de Sundance Kid vandaag de dag een bank zouden proberen te beroven. De veronderstellingen van waaruit ze dat 150 jaar geleden deden, zijn nu volledig achterhaald. Naarmate elektronisch bankieren toeneemt, hebben banken steeds minder contant geld in huis. De grootste kans op diefstal is tegenwoordig niet een gewapende bankroof, maar identiteitsdiefstal, diefstal van bedrijfsgeheimen op onbeveiligde iPads in taxi's en allerlei geavanceerde cyberbedreigingen.

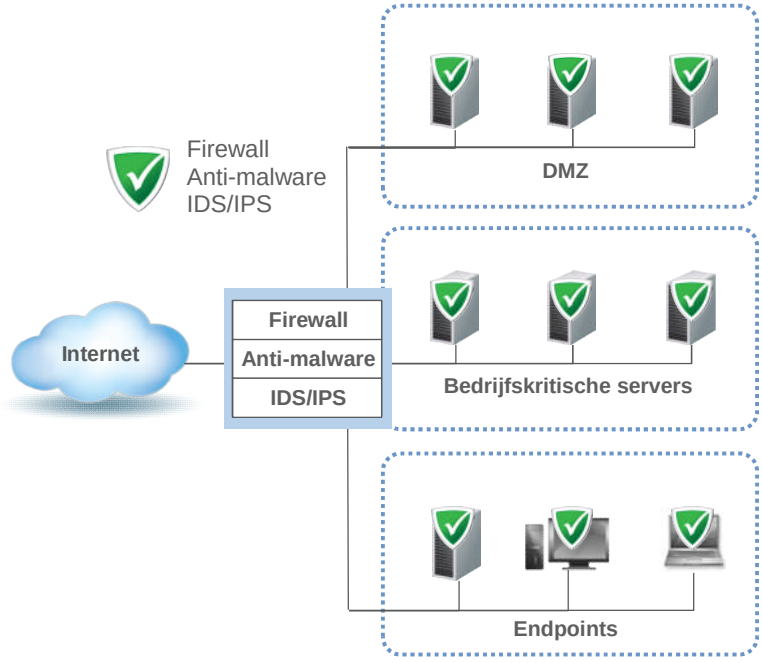
De trend in de richting van virtualisering en cloud computing is een van de belangrijkste oorzaken van deze paradigmaverschuiving. Ondernemingen stappen over op virtualisering en cloud computing,

omdat dit allerlei voordelen met zich meebrengt, zoals IT-flexibiliteit, schaalbaarheid, efficiëntie, kostenbesparing en concurrentievoordeel. Een recent rapport van Gartner stelt het volgende: "Virtualisering zal tot en met 2015 de grootste uitdaging blijven op het gebied van infrastructuur en bedrijfsvoering. Hierdoor verandert hoe u leiding geeft, hoe en wat u koopt, hoe u middelen inzet, hoe u plant en wat u in rekening brengt. Virtualisering zorgt ook voor een ommekeer op het gebied van licenties, prijsstelling en componentbeheer." [1] De omvang en het belang van deze trend betekenen dat beter moet worden gekeken naar de impact en de rol van beveiliging op het gebied van virtualisering en cloud computing.

III. TRADITIONELE NETWERKEN EN BEVEILIGING

Voor een goed begrip van de uitdagingen en kansen die virtualisering en cloud computing bieden, is het nuttig eerst te bekijken hoe beveiliging is geëvolueerd van traditionele netwerken naar de netwerken van tegenwoordig, en hoe deze evolutie waarschijnlijk verder zal gaan als gevolg van virtualisering en cloud computing.

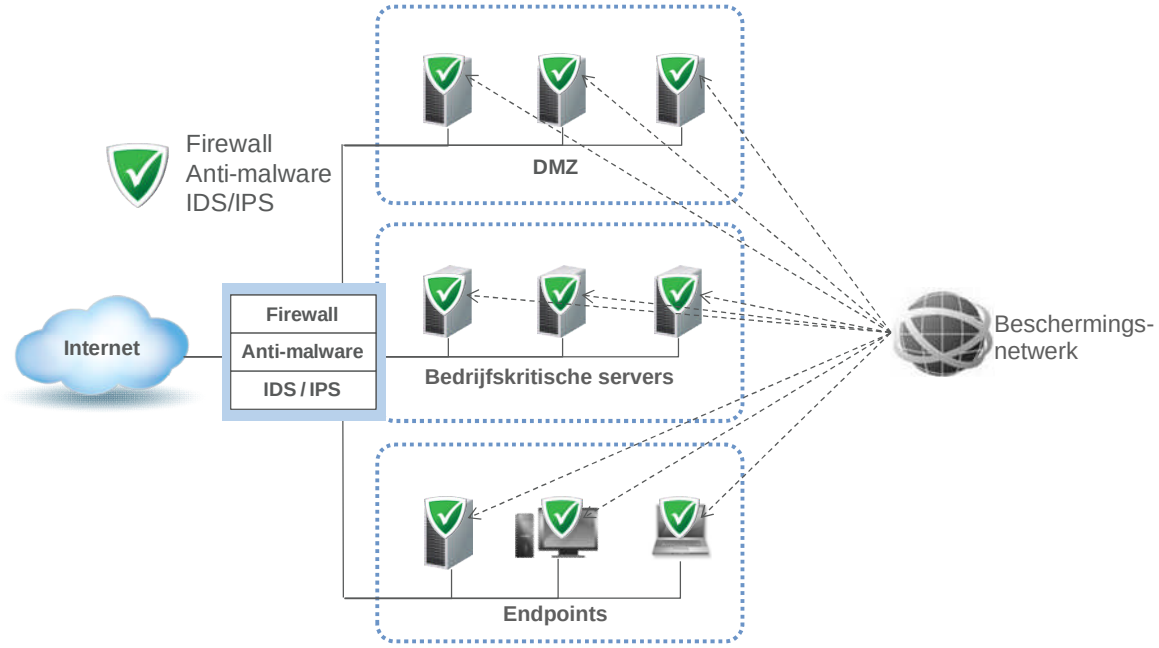
Afbeelding 1 toont een traditioneel netwerk met drie hoofdtypen computerresources binnen de buitengrenzen: computerresources in de DMZ, bedrijfskritische servers en endpoints. De relatief eenvoudige beveiliging bestaat uit firewalls, web- en e-mailbeveiliging en inbraakdetectie- en -preventiesystemen (IDS/IPS) aan de buitengrenzen van het netwerk. Host-based beveiliging bestaat uit anti-malware agents op elke computer binnen het netwerk.



Afbeelding 1. In een traditioneel netwerk bestaan host-based beveiligingsagents op elke machine vooral uit anti-malware, terwijl de beveiliging aan de buitengrenzen bestaat uit een firewall, web- en e-mailbeveiliging en IDS/IPS.

EEN HEERLIJKE NIEUWE BEVEILIGINGSWERELD: HOE BEVEILIGING VERANDERT OM VIRTUALISERING EN CLOUD COMPUTING TE ONDERSTEUNEN

Aangezien hackers een manier vonden om de beveiliging aan de buitengrenzen van het netwerk te omzeilen en er ook meer bedreigingen van binnenuit optraden, zagen klanten de noodzaak van diepgaandere bescherming op alle apparaten binnen het netwerk (zie afbeelding 2). Opdat de hosts konden zichzelf verdedigen, werden DMZ-resources, servers en endpoints uitgerust met firewalls en IDS/IPS's. Ongeveer tegelijkertijd werd de definitie van het endpoint opgerekt door de komst van nieuwe apparaten. Ondernemingen stonden steeds meer toe dat werknemers verbinding met het netwerk maakten vanaf hun laptop. Netwerken moesten hiervoor worden uitgebreid. Deze endpoints bewogen zich regelmatig buiten het netwerk en maakten dan weer opnieuw verbinding. Dit vroeg om een veerkrachtig soort beveiliging. De agents die op al deze apparaten binnen het netwerk waren geïnstalleerd (met toegang op afstand), moesten regelmatig worden bijgewerkt door een of ander type beschermingsnetwerk en gecentraliseerd beheer.

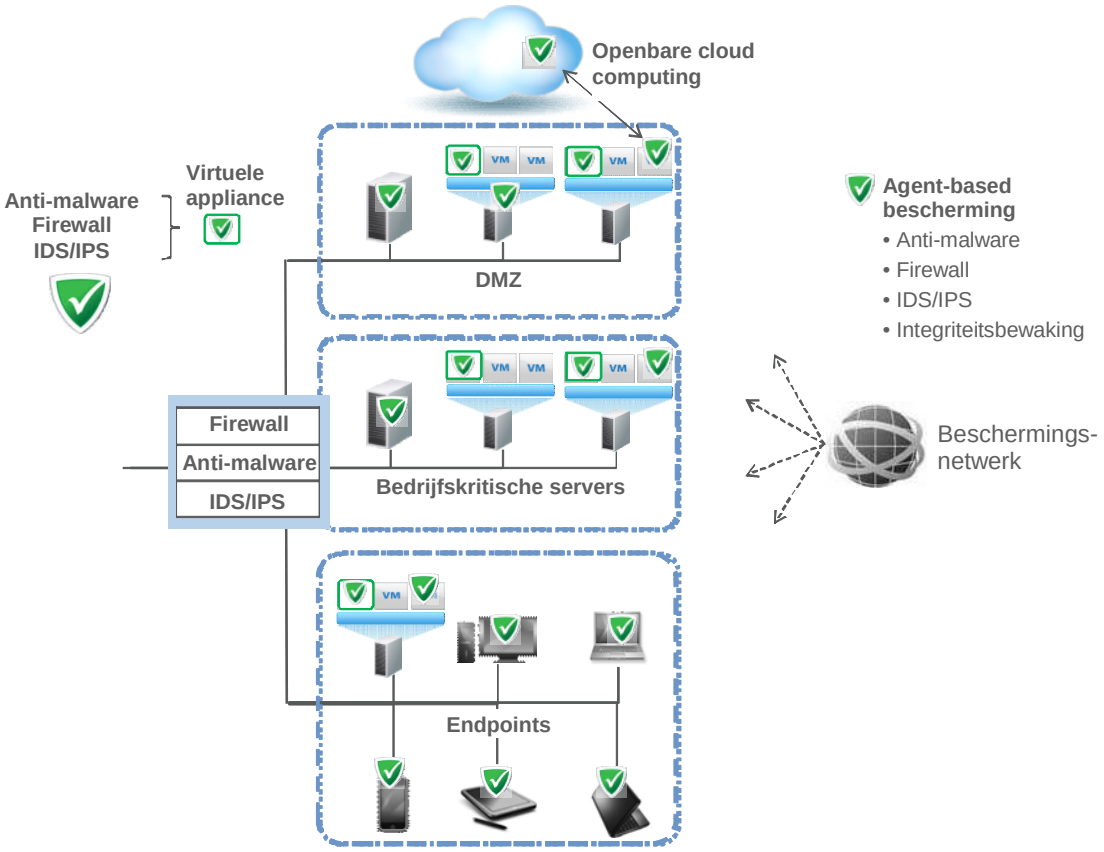


Afbeelding 2. In veel hedendaagse netwerken bieden hostagents diepgaandere bescherming. Netwerken zijn uitgebreid met mobiele endpoints of endpoints op afstand en er is een beschermings-netwerk geïmplementeerd.

IV. VIRTUALISERING

Door virtualisering wordt het traditionele netwerkmodel minder relevant, omdat migratie en uitdijing toepassingen en gegevens dynamischer maken en chokepoints in netwerken verdwijnen. Met het verdwijnen van de buitengrenzen moet de beveiliging nu helemaal doordringen tot aan elk logisch hostknooppunt, waar dat knooppunt zich ook bevindt.

De agents voor hostbeveiliging leveren diepgaandere beveiliging en kunnen zich met het computervermogen mee verplaatsen. Naarmate ondernemingen overstappen op virtualisering, wordt de inzet van een agent voor hostbeveiliging op alle hosts echter complexer. Het is lastig de snelle bewegingen van deze virtuele servers en desktops bij te houden.



Afbeelding 3. Naarmate organisaties meer overstappen op virtualisering, wordt het traditionele netwerkmodel minder relevant en moet de beveiliging worden uitgebreid naar elk logisch hostknooppunt. In deze afbeelding wordt de beveiliging met een virtuele appliance uitgebreid tot VM's.

Wanneer virtualisering wordt geïmplementeerd, voegen organisaties in eerste instantie virtuele machines (VM's) aan traditionele, fysieke machines toe in een hybride opstelling, zoals in afbeelding 3. Voor het leveren van de benodigde beveiliging heeft de onderneming een virtuele

appliance nodig – een software-image bestemd voor een virtuele machine. Door deze appliance in te voeren, kunnen organisaties in de hypervisor zelf beveiliging aanbrengen om effectievere bescherming te bieden. Hierdoor ontstaat ook overzicht over het verkeer tussen VM's en ontstaan andere beveiligingsvoordelen die specifiek zijn voor virtualisering, zoals beveiliging tussen VM's, virtuele patching voor hosts die worden gemaakt, en een efficiëntere werking van anti-malwaremodules.

De virtuele appliance wordt ingezet om alle VM's erachter te beschermen. Elke fysieke machine werkt nu bijna als een netwerk. Aangezien organisaties de neiging hebben soortgelijke toepassingen op dezelfde fysieke machines te plaatsen, biedt de inzet van een virtuele appliance organisaties de mogelijkheid meer granulaire beveiligingsregels in te stellen op dat virtuele punt, vergeleken met de algemene beveiligingsregels aan de buitengrenzen van het datacenter. Hierdoor kunnen ook firewall-/IDS-/IPS-regels aan de buitengrens gemakkelijker worden aangepast. Tegelijkertijd maakt deze configuratie 'agentless' bescherming voor het gehele virtuele netwerksegment mogelijk. Dit verbetert de prestaties van de algehele structuur en biedt noodzakelijke beveiliging als de agent voor host-beveiliging nog niet is ingezet of ontbreekt vanwege een platformbeperking. De virtuele appliance voor de beveiliging kan tevens de NAC-functie leveren (Network Admission Control); de appliance kan een beheerder informeren of waarschuwen, of voorkomen dat een VM die niet de juiste beveiligingsbehandeling heeft ondergaan, op een server wordt gestart of ernaar wordt verplaatst.

Naarmate het datacenter wordt geconsolideerd, richt het nieuwe beveiligingsmodel zich derhalve verder op verdediging in de diepte, waarbij het volgende gebeurt:

1. De buitengrenzen, zoals de traditionele firewall/IDS/IPS, worden nog altijd in de frontlinie beveiligd, waarbij vooral wordt verdedigd tegen aanvallen van buiten naar binnen – pogingen om de eerste verdedigingslinie van buitenaf te doorbreken.

2. Virtuele appliances in het virtuele netwerk verwerken meer granulaire beveiligingsregels, vooral met betrekking tot toepassingsbeveiliging en virtuele afscherming. Dit verbetert niet alleen de beveiliging van de buitengrenzen, maar zorgt ook dat er minder vaak wijzigingen hoeven te worden aangebracht op apparaten aan die buitengrenzen. Deze laag biedt ook noodzakelijke beveiliging in gevallen waarin geen agent voor hostbeveiliging is ingezet.

3. Host-based beveiligingsagents op alle hosts detecteren en wijzigen de beveiligingsrichtlijnen dynamisch als de computerwerklast verschuift, bijvoorbeeld van binnen in het ondernemingsnetwerk naar buiten het ondernemingsnetwerk, of naar een ander datacenter of de cloud.

EEN HEERLIJKE NIEUWE BEVEILIGINGSWERELD: HOE BEVEILIGING VERANDERT OM VIRTUALISERING EN CLOUD COMPUTING TE ONDERSTEUNEN

Deze aanpak vereist 'dial-it right' beveiliging. Een 'dialed-up' beveiliging slokt veel systeemresources en IT-medewerkers op; bij 'dialed-down' beveiliging is er minder bescherming maar zijn er ook minder systeemresources en IT-medewerkers nodig. Bij het bepalen van het beveiligingsniveau moet rekening worden gehouden met voorschriften, met de mate van vertrouwelijkheid van de gegevens en met beveiligingsrichtlijnen. Van geval tot geval het juiste evenwicht zoeken is gemakkelijker naarmate de bescherming dichter bij de eindbestemming van het inkomende verkeer wordt geïmplementeerd. De reden is dat voor beveiliging aan de buitengrenzen al het verkeer moet worden gescand dat het netwerk binnenkomt, een lastige taak omdat verschillende soorten verkeer, zoals op Linux, UNIX en Microsoft Windows gebaseerd verkeer, om verschillende redenen op weg zijn naar verschillende delen van het netwerk. Als echter dichter bij het doel wordt gescand, kan granulairder worden gescand, omdat alleen bepaalde soorten verkeer bedoeld zijn voor het doel. Zo is Linux-verkeer alleen bedoeld voor het Linux-platform. Hierdoor kan scannen door een virtuele appliance efficiënter zijn; de virtuele appliance bevindt zich dichter bij de bestemming dan een apparaat dat scant aan de buitengrenzen.

Radicale transformatie bij het endpoint

Virtualisering leidt tot een radicale transformatie bij het endpoint. Voordat er sprake was van virtualisering, was de activiteit van een gebruiker gekoppeld aan één fysiek desktop- of laptopknooppunt, dat werd beveiligd door een geïnstalleerde agent. Tegenwoordig hebben we te maken met desktopvirtualisering, waarbij de desktop in het datacenter draait. De veranderingen op het gebied van de desktop gaan echter veel verder dan het overbrengen van het besturingssysteem (OS) en de toepassingen van de desktop naar een VM in het datacenter. De desktop wordt omwille van inbraakdetectie en -preventie op de backend gedisassembleerd: het besturingssysteem, de toepassingen en de gebruikerspersona's worden apart beheerd en opgeslagen. Via het netwerk wordt alles op het moment van aanmelding weer gecombineerd tot de vertrouwde werkruimte voor elke gebruiker. Het besturingssysteem wordt verder ontmanteld tot basisimages die gebruikers gemeen hebben, en 'delta's' die uniek zijn voor elke gebruiker. Toepassingen mogen lokaal lijken, maar worden gestreamd naar de werkruimte en draaien in werkelijkheid op een andere VM of als SaaS-toepassing (Software as a Service) in de openbare cloud.

Deze werkruimte wordt nu gebruikt door een fysieke client die zich steeds meer op afstand bevindt en mobiel is. De trend die begon met thin terminals, breidt zich uit naar iPads en andere tablets, smartphones en 'Build Your Own' (BYO) pc's. Doordat de virtuele desktop vanaf meerdere locaties en apparaten toegankelijk is, is de werkruimte van de gebruiker overal en altijd beschikbaar. De desktop is nu mobiel, alomtegenwoordig, thin en heterogeen.

De gebruikerssessie definieert nu de desktop, omvat meerdere netwerklocaties binnen het datacenter en strekt zich verder uit over het WAN. Daarom kan een agent zich niet meer op één locatie bevinden en van daaruit de desktop beveiligen. Endpointbeveiliging moet nu meerdere netwerklocaties omvatten.

V. CLOUD COMPUTING

Virtualisering is een katalysator voor cloud computing; als gevolg van virtualisering worden data-centers bijvoorbeeld versneld getransformeerd tot besloten clouds. Naarmate organisaties meer gebruik maken van cloud computing, kunnen ze toepassingen verplaatsen van hun eigen resources naar resources in de cloud en weer terug, net wat het grootste voordeel biedt.

Deze manier om computervermogen te gebruiken, betekent wel een extra belasting voor het beveiligingsmodel. Zoals al gezegd, zijn er agents nodig die met de werklast meebewegen; dat omvat het besturingssysteem, toepassingen en gegevens. Zakelijke vereisten, zoals strikte naleving van de voorschriften, vragen echter om slimmere 'smart' agents die het beveiligingsniveau kunnen aanpassen aan de verschillende taken. Ondernemingen moeten aan steeds meer voorschriften en standaarden voldoen, zoals de Payment Card Industry Data Security Standards (PCI DSS), de Health Insurance Portability and Accountability Act (HIPAA) en de Gramm-Leach-Bliley Act (GLBA). Daarnaast zijn er controleprotocollen, zoals het Statement on Auditing Standards (SAS70) en ISO-standaarden (International Organization for Standardization). Ondernemingen moeten bewijzen dat ze voldoen aan beveiligingsstandaarden, ongeacht de locatie van gereguleerde systemen, inclusief servers op de eigen locatie, virtuele machines op de eigen locatie en virtuele machines op externe locaties, die draaien op cloud computing-resources.

Hierdoor zijn anti-malware, firewalls en IDS/IPS niet voldoende voor agent-based bescherming (zie afbeelding 3). Sommige van de hierboven genoemde voorschriften omvatten vereisten op het gebied van versleuteling ter beveiliging van kritieke gegevens, zoals creditcardgegevens en op personen herleidbare gegevens. Deze vereisten kunnen bestaan uit naleving van Full Disk Encryption (FDE), Advanced Encryption Standard (AES) en Federal Information Processing Standards (FIPS) 140-2. Aangezien de cloud met anderen wordt gedeeld, worden deze vereisten nog belangrijker. Integriteitsbewaking van kritieke bestanden van besturingssystemen en toepassingen is ook nodig om schadelijke of onverwachte wijzigingen te detecteren die zouden kunnen wijzen op aantasting van computerresources. Logboekinspectie is van belang om overzicht te bieden over belangrijke beveiligingsgebeurtenissen die in logbestanden op cloudresources kunnen ondersneeuwen. Tabel 1 laat zien dat de controlemechanismem die bij de traditionele benadering van beveiliging worden gebruikt, ook nodig zijn in de nieuwe, hybride cloudomgeving.

EEN HEERLIJKE NIEUWE BEVEILIGINGSWERELD: HOE BEVEILIGING VERANDERT OM VIRTUALISERING EN CLOUD COMPUTING TE ONDERSTEUNEN

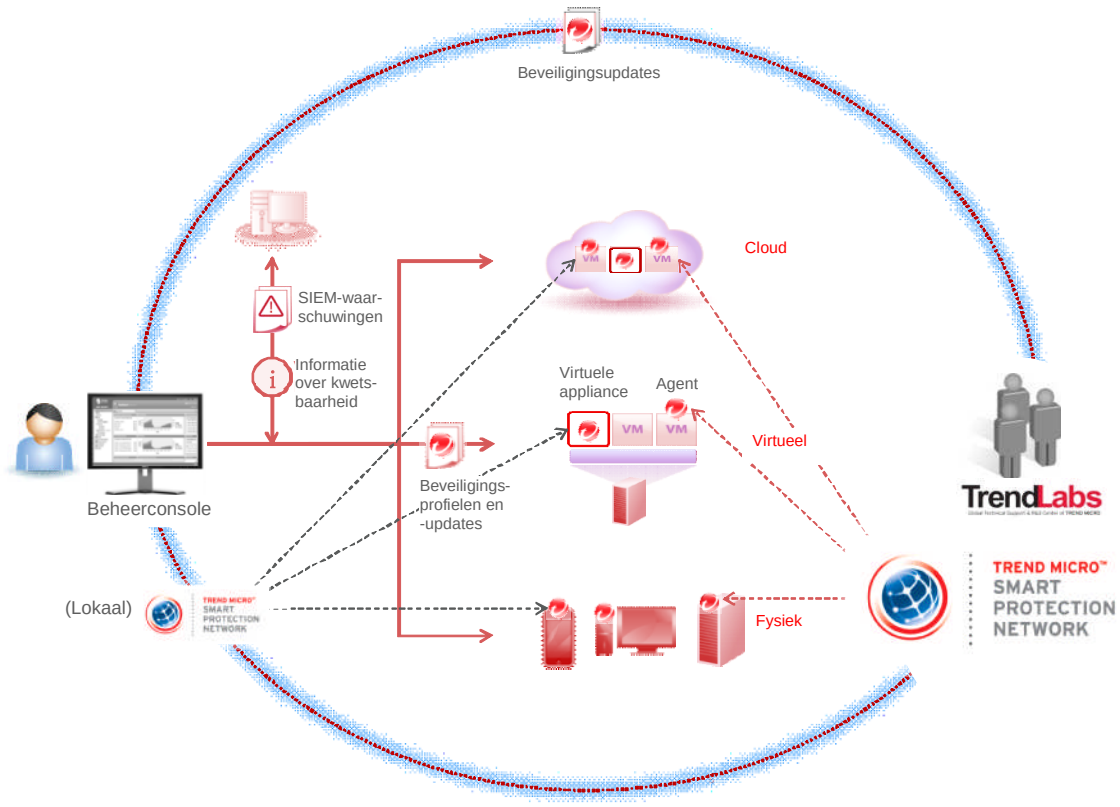
Controlemechanisme beveiliging	Traditioneel netwerk: (ommuurde tuin)	Nieuw netwerk: (hybride cloud)
Firewall	✓	✓
IDS/IPS	✓	✓
Bescherming voor webtoepassingen	✓	✓
Integriteitsbewaking bestanden	✓	✓
Logboekinspectie	✓	✓
Anti-malware	✓	✓
Versleuteling	✓	✓
Berichtenverkeer	✓	✓

Tabel 1. De controlemechanismen die bij de traditionele benadering van beveiliging worden gebruikt, zijn ook nodig in de nieuwe, hybride cloudomgeving.

VI. DE VISIE VAN TREND MICRO

Voor effectieve beveiliging in het tijdperk van virtualisering en cloud computing moeten oplossingen van de volgende generatie een optimale combinatie bevatten van methoden om traditionele, fysieke resources, virtuele resources en werklast te beschermen, ongeacht waar ze zich bevinden, met inbegrip van de cloud (zie afbeelding 4). Het Trend Micro Smart Protection Network™ biedt overzicht en zorgt ervoor dat de bescherming van resources en werklast door agents flexibel werkt en up-to-date is. Beveiliging beweegt indien nodig met de werklast mee en wordt op de hypervisor ingezet om alle gastbesturingssystemen vanuit één locatie te beschermen.

EEN HEERLIJKE NIEUWE BEVEILIGINGSWERELD: HOE BEVEILIGING VERANDERT OM VIRTUALISERING EN CLOUD COMPUTING TE ONDERSTEUNEN



Afbeelding 4. De visie van Trend Micro met betrekking tot beveiliging van de volgende generatie omvat een optimale combinatie van methoden om traditionele, fysieke resources, virtuele resources en werklast te beschermen, ongeacht waar ze zich bevinden, met inbegrip van de cloud.

De host biedt het grootste deel van de benodigde beveiliging in een gevirtualiseerde omgeving en uiteindelijk een cloud computing-omgeving. Deze host-based controlemechanismen vertegenwoordigen de virtualisering van beveiliging. Dat betekent om te beginnen dat beveiliging opgewassen moet zijn tegen instant provisioning, een van de grote voordelen van virtualisering. Dit kan echter kansen bieden: een eenmaal gedefinieerde beveiligingsrichtlijn kan direct worden geïmplementeerd zodra een nieuw apparaat wordt toegevoegd. Dit is een voorbeeld van hoe virtualisering grote en interessante kansen op verbetering van de beveiliging biedt. Deze evolutie van beveiliging biedt ook de mogelijkheid uitval als gevolg van infectie of een inbreuk op de beveiliging te voorkomen, wat de continuïteit van de bedrijfsvoering garandeert en helpt bij de naleving van voorschriften.

In dit door de host gedomineerde paradigma zijn leveranciers van beveiliging die ervaring hebben met het ontwerpen en implementeren van host-based beveiliging in het voordeel bij het aanbieden van deze uitgebreide en verbeterde beveiliging aan organisaties. Het ontwerpen van beveiliging voor grote aantallen hosts en endpoints is een heel ander verhaal dan het ontwerpen van beveiliging voor een netwerk. Leveranciers met uitgebreide ervaring op het gebied van de specifieke eisen en kansen van host-based beveiliging, en met het ontwikkelen van best practices op dit terrein, gaan waarschijnlijk de toonaangevende beveiliging van de nieuwe generatie leveren.

Door deze verandering zullen IT-budgetten anders aan beveiliging besteed gaan worden; er zal geleidelijk aan meer aandacht en geld gaan naar host-based beveiliging. Deze verschuiving zal echter niet van de ene op de andere dag plaatsvinden. De migratie van firewalls naar de desktop heeft ongeveer tien jaar geduurd; de evolutie van traditionele netwerken naar virtualisering en vervolgens naar cloud computing zal ook tijd in beslag nemen.

VII. KENMERKEN VAN EEN BEVEILIGINGSSTRATEGIE VAN DE VOLGENDE GENERATIE

Trend Micro levert een beveiligingsstrategie van de volgende generatie – een strategie waarmee ondernemingen maximaal kunnen profiteren van de voordelen en de kostenbesparing van virtualisering en cloud computing. Op het moment zijn de volgende elementen commercieel verkrijgbaar:

- **Cloudarchitectuur:** Beveiliging moet helemaal opnieuw worden opgebouwd om te worden geïntegreerd met en te profiteren van technologie en modellen voor virtualisering en cloud computing.
- **Mobiliteit:** In een wereld die steeds mobieler wordt, met 3G-netwerken, vMotion en cloud computing, en de grootschalige acceptatie van IT-producten als smartphones en tablets, moet beveiliging ook mobiel worden. De beveiliging moet meereizen met de gegevens, de toepassingen en de apparaten die erdoor worden beschermd.
- **Thin endpoint:** Endpointbeveiliging moet zo compact mogelijk zijn om te kunnen passen op kleine, thin apparaten als virtuele machines, smartphones en USB-apparaten, en moet weinig resources (geheugen, CPU-tijd, I/O) opslokken.
- **Snelheid:** Gezien het tempo waarin nieuwe bedreigingen en kwetsbaarheden worden ontdekt en de snelheid waarmee virtuele machines kunnen worden toegevoegd of worden overgezet van een inactieve naar een actieve staat, moet beveiliging moet snel kunnen worden aangebracht en bijgewerkt, en daarnaast de systeemprestaties zo min mogelijk aantasten.
- **Eenvoud:** Beveiliging moet eenvoudig te bedienen zijn, moet gemakkelijk met bestaande oplossingen en IT-infrastructuur kunnen worden geïntegreerd en moet automatisering, meldingen, rapportage en andere voorzieningen bevatten die beheer- en onderhoudstijd verminderen.
- **Reikwijdte van de bescherming:** Er moet een uitgebreide reeks essentiële controlemechanismen voor de beveiliging worden gevirtualiseerd, waaronder antivirus, versleuteling, DLP (Data Loss Prevention), firewalls, IDS/IPS, integriteitsbewaking voor bestanden en logboekinspectie, die probleemloos moeten werken in gevirtualiseerde omgevingen en cloud computing-omgevingen. Oplossingen voor de beveiliging van afzonderlijke punten zijn niet voldoende.

- **Effectieve, toegankelijke, ondersteunde en aan voorschriften voldoende bescherming:** Gezien de grootschalige verspreiding en de 'buy-your-own-computer'-modellen moeten beveiligingsoplossingen zowel overal beschikbaar zijn als gemakkelijk toegankelijk zijn voor consumenten, effectieve bescherming bieden, voldoen aan IT-standaarden voor ondernemingen en wereldwijd worden ondersteund.

- **Richtlijnen en controlemechanismen:** De meeste ondernemingen zullen voorlopig een hybride model moeten ondersteunen met fysieke resources, virtuele resources en cloud computing-resources. Beveiligingsrichtlijnen en controlemechanismen moeten consistent beschikbaar zijn en in al deze verschillende omgevingen werken.

VIII. OPLOSSINGEN VAN TREND MICRO

Met geavanceerde oplossingen die specifiek zijn ontworpen om deze omgeving te beveiligen, kunnen risico's worden verkleind, prestaties worden verbeterd, het beheer worden vereenvoudigd en uiteindelijk de beveiliging van datacenters worden voorbereid op de toekomst. Trend Micro levert beveiliging die is ontworpen voor virtualisering en cloudomgevingen. Trend Micro is toonaangevend op het gebied van gegevensbeveiliging met geavanceerde technologie zoals het Trend Micro Smart Protection Network™ en oplossingen die de continuïteit van de bedrijfsvoering en naleving van voorschriften garanderen. Trend Micro biedt op dit terrein de volgende oplossingen:

- Trend Micro™ Deep Security levert geavanceerde bescherming voor systemen in het dynamische datacenter, van virtuele desktops tot fysieke servers, virtuele servers en cloudservers. Deep Security combineert inbraakdetectie, een firewall, integriteitsbewaking, logboekinspectie en anti-malware-voorzieningen in één centraal beheerde softwareoplossing voor de hele onderneming. De oplossing is inzetbaar in configuraties met agents (virtuele appliances) en zonder agents.

- Trend Micro™ SecureCloud™ is een gehoste oplossing voor het beheer van sleutels en gegevens-versleuteling, die is bedoeld voor de bescherming en controle van vertrouwelijke informatie die wordt ingezet in openbare en besloten cloud computing-omgevingen. SecureCloud is efficiënt en gebruikersvriendelijk en helpt naleving van voorschriften te garanderen. Het biedt bovendien de vrijheid om van cloudleverancier te veranderen zonder vast te zitten aan het versleutelingssysteem van één leverancier.

- Trend Micro™ OfficeScan™ levert bescherming voor virtuele en fysieke desktops binnen en buiten het ondernemingsnetwerk. Het is de eerste oplossing voor endpointbeveiliging in de branche die is geoptimaliseerd voor VDI (Virtual Desktop Infrastructure). OfficeScan versnelt de bescherming, vermindert het beslag op resources en past virtuele patching toe.

- De infrastructuur van het Trend Micro™ Smart Protection Network™ biedt geavanceerde cloud-bescherming waarbij bedreigingen in realtime worden geblokeerd voordat ze gebruikers bereiken. Het werkt op basis van een unieke cloud computing-architectuur en gebruikt een wereldwijd netwerk

van technologieën voor bedreigingssensoren, e-mail, web- en bestandsreputatie die in samenhang het aantal infecties aanzienlijk verlagen.

- Trend Micro™ Mobile Security beschermt smartphones en PDA's tegen gegevensverlies, infecties en aanvallen vanaf een centrale ondernemingsconsole die ook desktopbescherming kan beheren.

Beveiligingsproducten van Trend Micro hebben hun waarde bewezen en zijn betrouwbaar en gereed voor gebruik, zoals door derden is gecertificeerd. Ga voor meer informatie naar www.trendmicro.com/virtualization.

IX. VOLGENDE STAPPEN

Ondernemingen die hulp zoeken bij de ondersteuning van hun initiatieven op het gebied van virtualisering en cloud computing, moeten hun leveranciers de volgende belangrijke vragen stellen:

- Hoe en sinds wanneer ondersteunt de leverancier de meest recente API's van VMware en andere toonaangevende leveranciers voor de beveiliging van gevirtualiseerde omgevingen?
- Wat is de visie van de leverancier met betrekking tot de mobiele beveiliging voor consumenten? Beschikt de leverancier over oplossingen die bescherming bieden voor tablets, smartphones en andere mobiele apparaten?
- Hoe ziet de cloud-clientarchitectuur van de leverancier eruit? Hoe maakt de leverancier gebruik van cloud computing om effectievere bescherming te bieden?

De overgang naar virtualisering en vervolgens naar cloud computing zal leiden tot hybride IT-configuraties, hetgeen kan leiden tot kwetsbaarheden en complexiteit op het gebied van beveiliging. Voor veel ondernemingen zal deze overgangsperiode vrij lang duren en daarom moeten ze nauw met een beveiligingspartner samenwerken om in alle fases van deze overgang te zorgen voor effectieve beveiliging. Deze leverancier moet zichzelf hebben bewezen op het gebied van host-based beveiliging, want beveiliging van virtualisering en cloud computing bevindt zich voornamelijk op de host, en moet blijk geven van een goed doordachte visie voor de toekomst.

X. CONCLUSIE

De IT-wereld verandert snel en consumenten/werknemers stappen in hoog tempo over op nieuwe mobiele apparaten. Alles draait om mobiliteit. Ondernemingen willen bovendien zo snel mogelijk profiteren van de voordelen van virtualisering en cloud computing. Beveiliging kan deze veranderingen mogelijk maken en kan ervoor zorgen dat ondernemingen profiteren van de potentiële voordelen. Beveiliging kan er ook voor zorgen dat de overgangsperioden soepel verlopen. De focus van beveiliging verschuift hierdoor van het netwerk naar de host. Trend Micro is al 22 jaar een toonaangevend leverancier van host-based technologie en is daarom de natuurlijke brancheleider in deze spannende tijd.

XI. VOOR MEER INFORMATIE

Ga voor meer informatie naar www.trendmicro.com/virtualization

XII. OVER TREND MICRO

Trend Micro Incorporated is wereldleider op het gebied van beveiliging van internetcontent en risicobeheer, streeft naar een wereld waarin ondernemingen en consumenten veilig digitale informatie kunnen uitwisselen. Als pionier op het gebied van antivirusproducten op serverbasis met meer dan 20 jaar ervaring, leveren we hooggewaardeerde beveiliging die voldoet aan de wensen en eisen van onze klanten, die nieuwe bedreigingen sneller tegenhoudt en die gegevens beschermt in fysieke omgevingen, virtuele omgevingen en cloudomgevingen. Onze toonaangevende technologie en producten voor de beveiliging van cloud computing werken met de infrastructuur van het Trend Micro™ Smart Protection Network™, houden bedreigingen tegen waar ze opkomen, op internet, en worden ondersteund door meer dan 1000 bedreigingsdeskundigen over de hele wereld. Ga voor meer informatie naar www.trendmicro.com.

Ga naar www.trendmicro.com.

XIII. REFERENTIE

1. “ATV: Virtualization Reality,” onderzoeksrapport van Gartner. Id-nummer G00205779, 30 juli 2010.