IPV6, NIET ALLEEN EEN LANGER ADRES!

Drs. Andor Demarteau CISA CISSP CEH is als Senior IT Security specialist de schakel tussen business en IT met een gefundeerde achtergrond in de techniek. Onderwerpen als PKI, encryptie, privacy, policies en procedures, risico analyses en security architectuur zijn de kernbegrippen binnen zijn vakkennis. In zijn vrije tijd is hij radiozendamateur en sportduiker. Andor is te bereiken via andor.demarteau@capgemini.com

Zeker 10 tot 15 jaar geleden toen het internet in opkomst was in onze business wereld, riepen de wetenschappers en ingewijden al dat de IP adressen eigenlijk al bijna op waren. Niemand geloofde ze natuurlijk.

Feitelijk echter hadden zij gelijk en het feit dat het uiteindelijk nu echt zover is, heeft meer te maken met een aantal kunstgrepen die wij in de industrie hebben uitgehaald, dan dat er daadwerkelijk meer adressen beschikbaar zijn gekomen.
Kunstgrepen als het opknippen van klasse A en B adressen uit de oude IPv4 adres indeling en NAT (network address translation) hebben er voor gezorgd dat de daadwerkelijke uitputting van de IP versie 4 adressen op zich heeft laten wachten. Dit heeft echter wel een heel groot nadeel tot gevolg: nu het daadwerkelijk zover is dat de adressen echt op zijn, lopen we keihard tegen de grenzen van het internet aan.
En dan nog maar niet te spreken over het misbruik van NAT en andere soortgelijke technieken als security maatregel.
In dit artikel zal ik kort ingaan op de risico's die wij in de nabije toekomst tegen zullen komen, wanneer wij gaan overstappen op IP versie 6. Dat dit zal gebeuren staat als een paal boven water, wanneer en hoe precies valt te bezien. Ook het tijdsbestek waarin dit zal gebeuren zal zich uitstrekken over het grootste zo niet het gehele huidige decennium.

Today's latte, World IPv6 Launch (Bron: Yuko Honda, via Flickr)

Wat is IP versie 6?
De naam, of liever de nummering, zou kunnen doen vermoeden dat het hier gaat om een upgrade van het huidige IP protocol (IP versie 4) en dat het puur gaat om alleen langere adressen zodat we weer een tijdje voort kunnen. Als het aan de industrie had gelegen was dat waarschijnlijk wel de uitkomst geweest. Echter, niet 15 maar al ruim 22 jaar geleden, hebben de wetenschappers ingezien dat het gebruik van het toen nog relatief nieuwe IPv4 protocol zijn problemen bezat, waarvan eentje, de lengte en opdeling in klassen van de adres ruimte, de meest urgente leek te gaan

worden richting het einde van de vorige eeuw.
In het steeds maar uitdijende internet bleek de opzet van het huidige IP protocol nog meer haarscheurtjes te vertonen die schreeuwden om een oplossing. Zo werd routering een steeds groter en complexer probleem en kwamen er langzaam ook vormen van misbruik aan het licht waarbij routering, fragmentatie van pakketten halverwege hun transport et cetera werden misbruikt.
De ontwerpers van het nieuwe IP protocol (IP versie 6) gingen met hun kennis en inzicht een flinke stap verder dan zij strikt genomen hadden moeten doen. Ze breidden de adresruimte uit van 32 naar 128 bits per adres, versimpelden de routeringsmechanismen dusdanig, dat aan een adres valt te zien waar dit in de wereld thuishoort, bouwden beveiligingsmechanismen als encryptie en authenticatie in het protocol in, verwijderden mogelijkheden tot het aangeven van routeringspaden en verboden het fragmenteren van IP verkeer en route.
Natuurlijk is er in de 20 jaar nadat de eerste RFCs (request for comments) over IPv6 zijn uitgekomen nog wel het een en ander gewijzigd en aangepast vanwege voortschrijdend inzicht, maar dit is kort gezegd wel waar het hele verhaal om draait.

Loop ik nu al gevaar?
Het korte antwoord daarop is "ja".
Echter dit verdient natuurlijk wel wat meer uitleg en verduidelijking.
De industrie is langzaam wakker aan het worden en zich aan het beseffen dat de IP versie 4 adressen echt op zijn en ze dus iets moeten doen. Er zijn in bijvoorbeeld China al hotels waar je met een IPv4 only machine niet eens meer op het lokale internet kan, omdat zij al volledig IPv6 only omgeschakeld zijn, maar dat terzijde.
Veel apparatuur, firmware, besturingssystemen en andere software die wij in onze business tegenwoordig kopen, is inmiddels IPv6 ready. In vele gevallen zelfs IPv6 enabled by default, zonder enige vorm van beveiliging of policies die de hardware en software moeten beschermen tegen aanvallen en misbruik.

We lopen keihard tegen de grenzen van het internet aan

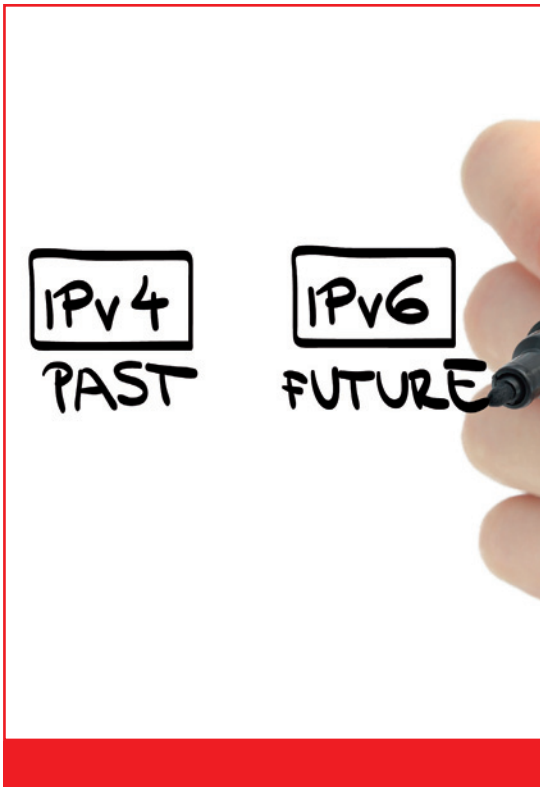
Laat nu dat precies het grootste probleem zijn in de huidige status van IP versie 6.
Het probleem zit hem in het feit dat IPv6 in tegenstelling tot zijn voorganger, het huidige IPv4, niet bepaald een simpele upgrade of uitbreiding is. Niet alleen de adressen zijn langer geworden, maar door de gehele opbouw van de IP protocolstack is er zoveel gewijzigd, dat als je IPv4 en IPv6 tegelijkertijd wilt kunnen gebruiken, je eigenlijk een duale oplossing nodig hebt. Je moet dus beide protocolstacks volledig naast elkaar draaien om beide soorten IP verkeer te kunnen afhandelen.
En dat is nu juist waar hier het probleem, of liever de uitdaging, zit. Beveiligingsmaatregelen genomen op de oude en vertrouwde IPv4 protocolstack gelden niet voor IPv6. Sterker nog, doordat IPv4 netwerken tegenwoordig veelal achter een NAT boundry zitten en deze dus deels worden misbruikt als security maatregel, ligt het IPv6 gedeelte van het netwerk volledig open en bloot.

Het IPv6 gedeelte van het netwerk ligt volledig open

Impact en risico
Zoals gezegd is veel van onze nieuwe apparatuur al IPv6 enabled en houden onze security policies, controls en maatregelen daar geen rekening mee. Dit gekoppeld aan het misbruik van NAT als security maatregel en het feit dat veel IPv6 enabled software zijn eigen lokale adressen al auto-configureert, zorgt voor een nogal gevaarlijke mix voor onze netwerk- en data beveiliging. Immers, als een hacker binnen wil dringen, komt hij niet langs de NAT firewall, want connecties naar binnen zijn niet mogelijk. Feitelijk correct.

Echter, gezien het feit dat uw firewall en routers inmiddels ook IPv6 praten, local-link adressen auto-configureren en je ook een IPv4 adres in IPv6 kan schrijven en daarmee je verkeer via de IPv6 stack kan laten lopen, is er een mooie en vooral "onzichtbare" route rond uw zo goed opgestelde firewall. Daar komt dan nog bij dat de meeste besturingssystemen, zoals Windows 7 en hoger, maar ook Mac OSX en Linux, precies hetzelfde doen. Nu hebben we een perfecte verbinding via het IPv6 enabled internet vanaf de hacker rechtstreeks tot in het hart van uw organisatie.
En voor wie denkt dat dit niet misbruikt kan worden of actief misbruikt wordt, zoek gerust zelf even op internet en je weet dat je al achterhaald bent.

Hoe is dit ontstaan?
Heel simpel, we zien dat de industrie eigenlijk nog steeds dezelfde fouten maakt die zij in het begin bij IPv4 ook maakten. "Och, leuke feature, maar daar is toch geen beveiliging voor



nodig?" Dezelfde fout die de industrie ook blijft maken voor consumenten en klein-zakelijke apparatuur zoals printers, scanners, multi-functionals, NAS en SAN storage drives, beveiligingscamera's etc. Security-by-design bestaat niet, kost geld en onze klanten willen er toch niet voor betalen als mijn concurrent het ook niet heeft en daardoor goedkoper is.
Deze wijze van werken strekt verder dan alleen netwerkbeveiliging, maar dat valt buiten de scope van dit artikel.
Het is belangrijk te onthouden dat uw leverancier van hardware en software uw veiligheid niet waarborgt, dat zult u als organisatie zelf moeten doen.
Dat geldt eens en temeer voor het hier aangegeven risico rond IP versie 6.

De oplossing

Echter er is niet echt een "de" oplossing, maar is het een traject met eerdere zijpaden die u kunt bewandelen. Dit heeft alles te maken met de keuze die u nu zult moeten maken: ga ik nu al investeren en kijken in hoeverre ik kan overstappen naar IPv6 of doe ik dat later. Het zal sterk van deze keuze afhangen wat uw verdere traject zal inhouden.

Ga ik nu al overstappen naar IPv6 of doe ik dat later?

Wat u echter te allen tijde zult moeten uitvoeren, is een risicoscan op uw huidige infrastructuur waarin u bepaalt wat er al wel en niet IPv6 enabled is, wat het beveiligingsniveau van uw systemen is als deze via IPv6 worden benaderd en wat u dient te doen om de beveiliging van deze systemen terug te krijgen op het door u gewenste niveau.
Dit is natuurlijk niet een eenmalige actie, maar zal moeten worden herhaald bij updates, upgrades en aanschaf van nieuwe hardware en software. Dit zal een integraal onderdeel van uw bedrijfsbeveiligingsstrategie moeten worden zolang u bezig bent of wacht op de transitie naar het IPv6 protocol. Immers, zolang die transitie nog niet is voltooid, zult u beide protocolstacks naast elkaar blijven gebruiken.

Hoe nu verder

De transitie naar IP versie 6 zal niet van de ene op de andere dag voltooid zijn, daarvoor zijn er teveel zaken die wijzigen en moeten worden aangepakt. Gedurende het hele traject blijft het risico dat de dualstack operation van IPv4 en IPv6 met zich meebrengt actief en vereist dit dus een verdeelde en dubbele aandacht op het gebied van infrastructuurbeveiliging.

Kunnen uw klanten u straks nog wel bereiken?

Wat de beste wijze van transitie is, zal sterk afhangen van uw organisatie. Als u veel oude apparatuur in uw infrastructuur heeft die het nieuwe IPv6 protocol niet aankan of over 5 tot 10 jaar toch zal worden vervangen door apparatuur die dat wel zou moeten kunnen (bijvoorbeeld SCADA systemen) dan maakt u waarschijnlijk nu de keuze de transitie voor die apparatuur nog niet te maken.

Daarnaast speelt mee in hoeverre straks het internet zelf, en uw service provider in het bijzonder, klaar zijn voor de toekomst.
En kunnen uw klanten u straks nog wel bereiken als u de switch wel maakt als een van de early adopters? Ook hierin zullen belangrijke keuzes moeten worden gemaakt en zal een dualstack oplossing in eerste instantie de enige mogelijkheid zijn.
Een aantal andere vragen die u zich zeker moet stellen zijn:

- hoe ga ik om met IPv6 only apparatuur in een IPv4 netwerk segment en vice versa
- wat doe ik met IPv6 verkeer van buiten mijn organisatie op mijn interne IPv4 intranet en vice versa
- hoe regel ik het huidige niveau van beveiliging in IPv6, zodat dit gelijk komt te staan of beter is dan mijn huidige IPv4 beveiliging?
- welke type van adressering ga ik gebruiken, en waarom en waar?
- welke apparatuur gebruikt welke klassen van adressering? (let op: meervoud)

In het algemeen kan worden gesteld dat IP versie 6 niet alleen als protocol een transitie heeft doorgemaakt, maar dat uw netwerk en uw beveiliging diezelfde transitie zullen moeten voltooien. Uw beheerders zullen niet meer hun systemen kunnen benaderen op basis van het IP adres dat ze altijd konden onthouden. Beveiliging en correcte adres resolving via DNS worden nog belangrijker en ongewenste gasten op uw netwerk, die hun "eigen" IP adres kunnen "kiezen", zullen nog lastiger op te sporen zijn.
En dan heb ik het nog maar even niet over alle mogelijke aanvalspaden en privacy issues die gerelateerd zijn aan deze nieuwe en toch oude technologische vooruitgang.
Kortom, werk genoeg. De vraag is namelijk niet of maar wanneer deze transitie zal worden ingezet, we kunnen niet anders en staan met de rug tegen de grenzen van het Internet gedrukt. ●