

Digitale toegang tot het

Met enige regelmaat hebben medewerkers vragen over hoe ze toegang kunnen krijgen tot het bedrijfsnetwerk. Vaak is er door het bos van de verschillende softwareoplossingen ook niet meer te zien welke manieren er zijn om die toegang te krijgen. Dit artikel probeert een licht te werpen op de verschillende soorten VPN's (Virtual Private Networks).

JAN FOLKERT BETHLEHEM *

Digitale toegang beschrijft manieren om toegang te krijgen van de ene computer tot een andere. Strikt gezien zou toegang via een seriële kabel of een netwerkkabel al kunnen worden gezien als digitale toegang. In dit artikel gaat het echter over manieren om toegang te krijgen vanaf een thuiscomputer naar een andere computer ergens op het internet. Dit kan een computer zijn van een kennis waarmee je samen een spel wilt spelen, maar in het kader van dit artikel betreft het met name een server in het bedrijfsnetwerk waarop bestanden staan die je nodig hebt.

VPN

Een VPN (Virtueel Particulier Netwerk of Virtueel Privénetwerk, Engels: Virtual Private Network) is een goedkope manier om een Wide Area Network (WAN) uit te bouwen met behoud van vertrouwelijkheid over een bestaande verbinding. Deze dienst maakt gebruik van een reeds bestaand netwerk, doorgaans het internet, om informatie-deling tussen geografisch afgescheiden netwerken mogelijk te maken. Het lijkt dan alsof er voor deze informatiedeling een *dedicated* netwerk voorzien is, terwijl er fysiek van een bestaand netwerk gebruik wordt gemaakt (Bron: Wikipedia).

Typen

Er zijn meerdere typen VPN om toegang te krijgen tot andere computers. Zo zijn er klassieke VPN's, zero-configuration VPN's, zogenaamde thuis-

werkplekken, 'directe verbindingen' en *portforwards*.

Klassieke VPN's

Klassieke VPN's zijn VPN-netwerken zoals die veelal door bedrijven worden gebruikt. Je neemt een server, installeert en configureert daar VPN-software op, en geeft aan de medewerkers een stukje extra software mee dat op het systeem thuis moet worden geïnstalleerd. Dit stukje software zet dan een virtueel netwerk op, waarmee de gebruiker toegang kan krijgen tot de servers. Voorbeeld hiervan is de software van Cisco, OpenVPN en Microsoft.

Zero-configuration VPN's

Zero-configuration VPN's zijn vergelijkbaar met normale VPN's, in zoverre dat zij ook een virtueel netwerk opzetten naar andere systemen. Het grootste verschil met klassieke VPN's is dat iedereen *clients* gebruikt en de server wordt beheerd door de maker van de zero-configuration VPN software. De beheerder regelt vervolgens alle configuraties en zorgt ervoor dat iedereen het juiste virtuele netwerk heeft. Voorbeeld hiervan is de software van LogMeIn, TeamViewer en N2N. TeamViewer heeft, in tegenstelling tot de andere twee, de mogelijkheid om *remote desktop* toegang te geven tot de pc.

Thuiswerkplekken

Thuiswerkplekken borduren vaak voort op de oude remote desktop omgevingen, waarbij met een stukje software een virtuele desktop op een server kan

worden verkregen. Het grote verschil is dat vaak in plaats van een extra stuk software alleen een webbrowser nodig is en dat de gebruikers naar een website moeten gaan, daar inloggen en dan een desktop in hun webbrowser krijgen. Voorbeelden hiervan zijn Citrix XenApp, NoMachine NX en OpenNX. NoMachine NX en OpenNX hebben eigen software nodig, maar Citrix heeft alleen een webbrowser met Java nodig.

Directe verbindingen en port forwards

Directe verbindingen en port forwards zijn de simpelste manieren om toegang te krijgen tot informatie op het werk. Zij zijn echter vaak ook het meest gelimiteerd en het lastigst te beveiligen. Er kan alleen toegang worden verkregen tot een poort op een server. Een website, al dan niet achter een firewall, is hiervan een voorbeeld. Het verschil tussen een directe verbinding en een port forward is dat bij een directe verbinding bezoekers met de machine zelf verbinden. Port forwarding wordt gebruikt als een server achter een router staat en de gebruiker feitelijk verbinding maakt met de router of firewall. De router stuurt dan het verkeer van de gebruiker door naar de server en het verkeer van de server terug naar de gebruiker.

Wanneer welke VPN?

De vraag is vervolgens wanneer welk type VPN wordt gebruikt. Maar eigenlijk is daar een relatief eenvoudig antwoord op te geven:

» Klassieke VPN's gebruik je als je

bedrijfsnetwerk

meerdere gebruikers toegang wilt geven tot het gehele netwerk en het systeem van de gebruiker volledig te vertrouwen is.

- » Zero-configuration VPN's gebruik je alleen tussen computers waarbij security geen hoge prioriteit heeft en snel en makkelijk een virtueel netwerk moet worden opgezet, zoals bijvoorbeeld voor computerspelletjes.
- » Thuiswerkplekken gebruik je als je meerdere gebruikers toegang wilt geven tot het gehele netwerk en alle daarop draaiende programma's, maar geen vertrouwen hebt in de computers van de gebruikers.
- » Directe verbindingen en port forwards gebruik je als je een dienst open wilt zetten voor iedereen op het internet.

Voor- en nadelen

Iedere techniek heeft natuurlijk voor- en nadelen. Zo ook de VPN's.

Klassieke VPN's zijn zeer veilig als de computers van de gebruikers dat ook zijn. Als een van de computers echter besmet is met een virus, kan die computer ook andere computers met virussen besmetten. Bij klassieke VPN's worden bij voorkeur 'dichtgetimmerde' pc's van de organisatie zelf gebruikt, die niet door de gebruiker kunnen worden gewijzigd. Privé-pc's zijn uit den boze.

Zero-configuration VPN's zijn ideaal voor het snel koppelen van twee of meer computers. Echter, het is vaak een klein aantal en de veiligheid van de verschillende computers is meestal niet bekend. Ook is er die derde partij, die de servers beheert. Daarvan bestaat geen 100 procent zekerheid dat zij het verkeer tussen de verschillende computers niet kan onderscheppen en af luisteren. Voor bijvoorbeeld TeamViewer is het niet verplicht om beheerrechten te hebben op de machine waarop de software draait. Hierdoor is het mogelijk dat gebruikers op het werk de software draaien en vanaf thuis toegang krijgen



tot de pc op het werk zonder tussenkomst van de beheerders van het netwerk. Blokkeren van zero-configuration firewalls is sowieso lastig: vaak worden HTTP-poorten gebruikt om naar buiten te verbinden met de centrale servers en moet in de firewall op IP-basis geblokkeerd worden, als de IP-adressen al te achterhalen zijn.

Thuiswerkplekken zijn veel veiliger dan de klassieke VPN's. Gebruikers kunnen alleen wat de beheerders toestaan en verder eigenlijk niet al te veel. Informatie komt niet op de thuis-pc terecht. Het nadeel is echter dat iedere gebruiker een eigen virtuele pc heeft, waardoor iedere verbonden gebruiker *resources* op de gedeelde server gebruikt. Een server kan vaak niet meer dan een tiental gebruikers aan voordat de gebruikers gaan klagen dat het werken wel heel erg traag wordt. Videobewerking en andere multimediale toepassingen zijn dikwijls ook niet te gebruiken.

Directe verbindingen en portforwards zijn het eenvoudigst op te zetten. Er hoeft alleen een server ingericht te worden en eventueel moet een poort op de firewall worden opengezet. Echter, doordat iedereen (dus ook hackers) vanaf het internet toegang kan krijgen tot (bijvoorbeeld) de website, moet de website heel goed programmatisch worden beveiligd. Dit kan worden gedaan door gebruikersnamen en wachtwoorden te gebruiken. De software mag echter geen bugs hebben die kunnen worden misbruikt (hackers zijn continu op zoek naar nieuwe servers die zij kunnen inzetten voor hun eigen doeleinden). «

* Jan Folkert Bethlehem is adviseur bij LBVD Informatiebeveiligers en betrokken bij projecten op het gebied van informatiebeveiliging met een uiteenlopend karakter, waaronder Penetratietests en MysteryGuest-acties.

Samenvatting

- » **Klassieke VPN's** zijn ideaal voor bedrijven die zeker weten dat de verbindende pc's veilig zijn.
- » **Zero-configuration VPN's** zijn ideaal voor low- en no-security omgevingen, zoals privécomputers.
- » **Thuiswerkplekken** zijn ideaal voor bedrijven die geen vertrouwen hebben in de pc's van de medewerkers en niet willen dat gegevens op deze pc's terecht komen.
- » **Directe verbindingen** zijn gemakkelijk voor beheerders, mits de software veilig en up-to-date is.