

Netwerken zien individuen

In moderne netwerken wordt toegangscontrole toegepast op basis van individuele kenmerken. De mogelijkheden die een gebruiker krijgt worden niet langer bepaald door de fysieke netwerkaansluiting, maar door zijn rechten conform een profiel. De gebruiker is niet langer gebonden aan een locatie. En beheerders zien nu overal identieke netwerkinstellingen. In draadloze netwerken kan de gebruikerslocatie mede bepalen welke mogelijkheden men heeft. We kunnen zelfs informatie naar de gebruiker sturen op basis van zijn locatie. Ook kan apparatuur snel worden teruggevonden op basis van locatiebepaling.

minder beheer, meer mogelijkheden, sterkere beveiliging

Traditionele situatie

In veel netwerken wordt nog op basis van fysieke aansluitingen bepaald welke systemen gebruikers kunnen benaderen, over welke bandbreedte ze beschikken, etcetera. Het netwerk is daardoor niet transparant en de beveiliging niet erg hoog. En als een werkstation met een virus wordt aangesloten, dan kan in korte tijd het hele netwerk besmet raken. Zowel moderne bekabelde als draadloze netwerken kunnen echter gebruikers herkennen. Het netwerk bepaalt dan dynamisch de mogelijkheden voor die gebruiker zolang deze actief is op de betreffende aansluiting. Tevens kan het netwerk vooraf controleren of het werkstation voldoet aan bepaalde eisen en of deze virusvrij is.

Nieuwe situatie

De overgang van een traditionele situatie naar een nieuwe situatie met individuele herkenning kan volledig gefaseerd en per aansluiting plaatsvinden. Hiervoor zijn een aantal componenten nodig, die in veel netwerken al aanwezig zijn. Om gebruikers te herkennen dienen zij opgeslagen te zijn in een centrale database. In veel gevallen is dit al gerealiseerd in een directory service, zoals Active Directory Service (ADS) of Novell

Directory Service (NDS). Om de netwerkapparatuur dynamisch te vertellen welke rechten een aansluiting moet krijgen, wordt een RADIUS server gebruikt. Ook deze is vaak al aanwezig om remote access en draadloze gebruikers toegang te verlenen. Tenslotte dienen de netwerkapparatuur en het werkstation het gestandaardiseerde IEEE 802.1x protocol te ondersteunen. Vrijwel alle draadloze en bekabelde netwerkapparatuur doet dat inmiddels. Via een speciale DNS/DHCP-appliance is echter ook een overgangsfase realiseerbaar.

De gebruiker

Om een gebruiker te herkennen dient deze zich aan te melden op het netwerk. Dit kan met een traditionele login en wachtwoord combinatie. Veiliger is om het wachtwoord te vervangen door een token of smartcard. Door USB-tokens en Single-Sign-On daarbij te combineren kan dit proces zowel zeer veilig als uiterst gebruikersvriendelijk plaatsvinden. Binnen een jaar zullen zelfs systemen beschikbaar zijn met een alles-in-één token/smartcard beheerapplicatie, waarbij ook fysieke toegangscontrole, biometrie en chipknip achtige kaarten zijn geïntegreerd. De gebruiker ziet bij individuele herkenning vrijwel geen

verschil meer tussen bekabelde netwerkaansluitingen, draadloze netwerken en de thuiswerkplek. En het netwerkbeheer wordt een stuk eenvoudiger.

Extra mogelijkheden

In draadloze netwerken is plaatsbepaling inmiddels een volwassen technologie geworden met vele mogelijkheden. Bijvoorbeeld beveiligings- en ziekenhuispersoneel kunnen snel gelocaliseerd worden bij calamiteiten. Dure apparatuur kan gevolgd en teruggevonden worden. En informatie kan worden aangeboden afhankelijk van de locatie. De meest geavanceerde systemen zijn zelfs in staat om te bepalen dat men binnen of buiten een ruimte staat. Tevens kan draadloze toegang volledig worden geblokkeerd vanaf locaties buiten het gebouw, een vaak gewenste extra veiligheidsmaatregel.

Uw partner

Als specialist is Vosko Networking BV een gedegen partner voor uw ICT-infrastructuur-, IP-telefonie- en beveiligingsoplossingen. Wij zijn actief sinds 1976 en verzorgen in Nederland beveiligde telefonie- en data-infrastructuren inclusief service en onderhoud voor vele grote bedrijven en instellingen. Wilt u meer weten? Bel of schrijf even.

Door: Wim Coenen